NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

DOD/DON REQUIREMENTS FOR
COMPUTER RISK ASSESSMENTS

by

Margaret A. Black

and

Martin F. Doherty

June 1983

Thesis Advisor: Norman R. Lyons

Approved for public release; distribution unlimited

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) DOD/DON Requirements for Computer Risk Assessments		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis June, 1983
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Margaret Anne Black Martin F. Doherty		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, Ca. 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS		12. REPORT DATE June, 1983
		13. NUMBER OF PAGES 92
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report)
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for Public Release; Distribution Unlimited

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Risk Assessments, Risk Analysis, Computer Security,

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The current methodology for conducting Computer Risk Assessments within the Department of the Navy is examined by studying the theories and philosophies that have evolved from the perspective of the Federal Government. A review of the Navy's attitude and procedures for both contractual Assessments is presented, along with a general framework for conducting an assessment of the computer systems at the Naval Postgraduate School. Attention is

(Continued)

ABSTRACT (Continued) Block # 20

then focused on the relative merits of automated and manual Risk Assessment methods, followed by an outline of proposed design specifications for a decision support system.

Approved for public release; distribution unlimited.

DOD/DON Requirements for Computer Risk Assessments

by

Margaret A. Black
Lieutenant, United States Navy
B.A., Bucknell University, 1975

and

Martin F. Doherty
Lieutenant, United States Navy
B.A., Holy Cross College, 1976

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
June 1983

ABSTRACT

The current methcdology for conducting computer Risk Assessments within the Department of the Navy is examined by studying the theories and philosophies that have evclved from the perspective cf the Federal Government. A review of the Navy's attitude and procedures for both contractual assistance and inhcuse approaches to conducting Risk Assessments is presented, along with a general framework for conducting an assessment cf the computer systems at the Naval Postgraduate School. Attention is then focused on the relative merits of automated and manual Risk Assessment methods, fcllowed by an outline of proposed design specificaticns fcr a decisicn support system.

TABLE OF CONTENTS

I. INTRODUCTION 9

II. DEPARTMENT OF DEFENSE/DEPARTMENT OF THE NAVY DIRECTIVES 16

A. GENERAL 16

B. GOVERNMENT CONCERNS 17

C. LEGISLATION 18

D. DEFINITIONS 21

E. FIPS PUB 31 METHODOLOGY 21

1. Estimating Loss 21

2. Evaluating Threats 26

3. Calculating the Annual Loss Expectancy (ALE) 28

F. SUBSEQUENT GOVERNMENT DIRECTIVES 30

G. FIPS PUB 65 METHODOLOGY 32

H. CURRENT DIRECTIVES 39

III. IN-HOUSE VS CONTRACTUAL SUPPORT 42

A. GENERAL 42

1. The Need for Contractual Support 43

2. A Prototype for a Contracted Risk Assessment 43

3. Standardization in Contracted Risk Assessments 44

4. Preliminary Efforts 44

5. The Contract 46

6. Future Risk Assessment Contracts 47

7. Proposal Evaluations and Selection 51

E. CONCLUSIONS 52

IV. A FRAMEWORK FOR CONDUCTING A RISK ASSESSMENT AT NPGS 55

A. INITIAL STEPS: PERSONNEL SELECTION AND SECURITY SURVEY 56

B. ASSET IDENTIFICATION AND VALUATION 59

C. THREAT AND VULNERABILITY EVALUATION PHASE . . 62

D. EVALUATION AND SELECTION OF ADDITIONAL COUNTERMEASURES 64

V. AUTOMATED VS. MANUAL RISK ASSESSMENT SYSTEMS . . . 67

A. GENERAL 67

B. A RISK ASSESSMENT AS A DECISION SUPPORT SYSTEM 69

C. DESIGN SUGGESTIONS FOR A DECISION SUPPORT SYSTEM 71

1. The Dialog Component 71

2. The Data Component 72

3. The Modeling Component 76

4. Integration of Components 76

D. LIMITATIONS 79

VI. CONCLUSIONS AND RECOMMENDATIONS 80

A. SUGGESTIONS/RECOMMENDATIONS FOR IMPROVEMENTS . 83

APPENDIX A: EXAMPLES OF VARIOUS FORMS USED IN RISK ASSESSMENT COMPUTATIONS 85

LIST OF REFERENCES 88

INITIAL DISTRIBUTION LIST 92

LIST OF TABLES

I. Loss Exposure 24

II. Sources for Threat Information 25

III. Estimating Fire Loss 29

IV. Orders of Magnitude of Estimated Impact and Frequency 34

V. Table for Selecting of Values of i and f 35

LIST OF FIGURES

2.1 Seismic Risk Map 27

2.2 Combined Matrix of i, f, and ALE 37

2.3 FIPS PUB 65 WORKSHEET 38

2.4 Time Line of Government Directives 41

3.1 DON/ADP security Organizational Relationships . 45

3.2 Small Business Matrix 50

3.3 Contractor Evaluation Score Sheet 53

4.1 Major Steps of Method I Risk Assessment 60

4.2 Sensitive Data Value Guidelines 61

5.1 Initial Screen for a Risk Assessment DSS 72

5.2 Bar Graph Output Representation 73

5.3 Field Layout for Required Files 75

5.4 Permanent Model Capabilities 77

5.5 Integration of DSS Components 78

I. INTRODUCTION

The advent of computer technology during the previous two decades has affected virtually every aspect of government and private industry. As technological advances foster the availability of complex systems at lower prices, the integration of computer systems with governmental and industrial processes is accelerated. Applications of computer systems range from relatively routine data processing tasks such as payroll, accounting packages, and inventory control to intricate scientific systems controlling space flights and decision support systems assisting managers in resolving unique problems.

The pervasiveness of this technology has created many new issues for management concern at all levels of government and industry. Among these issues is the subject of security. As systems become more and more complex, organizations which utilize them are becoming more and more dependent upon them. This relationship is forcing computer-center management to devote efforts toward improved security in all areas: hardware; software; communications; personnel; and administration [Ref. 1]. It is useful to consider exactly what we mean by the term "security" with respect to computer systems. According to Wylie, security is "a state of mind reached when one's assets are receiving appropriate protection. Protection has three facets of equal importance. Preventative techniques are applied to prevent the occurence of threats. Detection techniques are applied to ensure that all threat occurences are registered. Finally, for every threat occurence there must be an appropriate response." [Ref. 2] These definitions present a framework on which a computer system security plan may be

developed. It may not be possible to design a system which defeats every intrusion attempt. However, an adequate goal for many organizations might be to raise the cost of unauthorized or illegal use of a system to an amount so high that it discourages any attempts. While this goal is being pursued with vigor today, contemporary literature is replete with examples of computer crime. The U.S. Chamber of Commerce estimates that if computer abuse grows proportionally with the number of computers in operation, there will be roughly $160 million annual loss by 1985 [Ref. 3].

Government agencies at all levels and private enterprises, especially banks, must be concerned with the threat of sabotage and disruption, not only theft. The financial institutions participating in the electronic fund transfer sytem (EFTS) in the U.S. handle amounts of money equal to the national debt every four days [Ref. 4]. The potential for economic disaster of enormous magnitude exists. The motivation to prevent large-scale penetration and disruption of systems such as EFTS is providing impetus for security research.

The need for computer system security is self-evident. The magnitude of the problem is enormous. Partial solutions to this problem are being addressed in all areas. For example, software houses have developed sophisticated data access control packages. Many hardware vendors are including some type of security-control feature in their products. The issue of computer security, however, is not confined to technical considerations alone. Management must become intimately involved in this area if meaningful progress is to be made. A commitment by top management, clearly indicating to the entire organization the emphasis that must be placed upon security, is necessary. Management at all levels must be involved with determining policy and implementing measures concerning the organization of a

computer security program, security administration, risk assessments, personnel practices, and back-up, recovery and disaster planning.

The federal government, including both civilian and military agencies, is the largest user of ADP facilities in the country [Ref. 5]. Computer usage spans a vast diversity of applications such as World-Wide Military Command and Control System (WWMCCS), Social Security System, communications, federal payroll and accounting systems, etc. This immense usage has logically generated interest in the security of these particular computer systems. In fact, the attention being devoted to the security of computer systems is so great that the Office of Management and Budget established requirements in 1978 that, among other things, every agency implement a computer security program. OMB also defined a minimum set of controls to be incorporated into each agency's computer security program. [Ref. 6]

Contemporary literature on computer security seems to be in agreement in expressing the view that the best approach to computer security is the "total systems" approach. Critical areas which must be examined include hardware, software, users, programmmers, data, input/output documents, and procedures. Other facets of a system pertinent to a particular organization may also need to be examined. One element of the "total systems" approach is the conduct of a risk assessment.

What is a risk assessment? Many texts offer definitions which differ slightly in scope and degree. Perhaps the most concise and applicable is Peter Browne's definition: "A risk assessment is an analytic process designed to quantify the DP (data processing) security required by an organization. It considers the threats to information and the loss that would occur if a threat were to materialize." [Ref. 7] The results of a risk assessment enable an organization to

consider solutions to security problems which are cost-effective. The solutions may either attempt to reduce the probability of threats, lessen the effects of various threats, or aid in the recovery from a "successful" threat.

An organization may be able to conduct its own internal risk assessment if personnel assets are available. Specialists in computers, security, finance, personnel and operations will be required. Contracts may be utilized with one of several commercial companies organized to conduct, or to provide limited assistance, in risk assessments. Chapter Three will address this issue in depth. Of course, the active participation of management is crucial.

A risk assessment is a dynamic concept. It should be revised periodically to account for any changes in equipment, software, operating procedures, or any different element which might affect the overall security of the system. In particular, Naval activities with computer systems are required to update their risk assessments at least every five years [Ref. 8].

The federal government, as well as business enterprises, must approach the security problem in an economical manner. The risk assessment provides a logical framework to conduct a rational analysis. Management must provide guidelines to reach answers to the following questions:

1) What are the specific results required; how much security is required?
2) What is the proper balance between security program cost and potential benefits?
3) When tradeoffs can be made between protection and recovery, how much effort should be expended on each? [Ref. 9]

Obviously the minimum amount of security needed is to protect those items that are required to keep the organization operating. The security manager should incorporate

into the security plan those functions which are supported by computer facilities and essential to the continued operation of the organization. Additional elements may also be protected if it is economically feasible for the organization. A cost-benefit analysis may be applied to the decision-making process concerning additional security measures.

In a risk analysis situation, it is necessary to identify and assess the degree of threat against the computer resources of the organization. The degree of threat may determine the need for protection of some asset. The amount and cost of effort to be expended in examining particular threats should be proportional to the potential loss caused by such threats. Threats can usually be grouped into one or more of the following categories:

1) natural hazards and accidents such as fire, earthquakes, hurricanes, etc.
2) internal accidents and breakdowns such as programmer and operator errors, hardware failures, etc.
3) violent intentional actions such as sabotage, strikes, etc.
4) non-violent intentional actions such as fraud, embezzlement, and theft. [Ref. 10]

The potential loss associated with each threat must also be examined . Some consistent quantifying standard must be applied to each threat so that comparisons between losses can be made. Similar to threats, losses may also be grouped into four general categories:

1) delayed processing- the expense incurred when a computer application is not processed on time .
2) loss of data processing assets- these are the organizational assets in the custody of the data processing unit. Data are the most valued assets and loss of data may cause irreparable harm.

3) loss of organization assets by means of computer applications-when assets such as accounts receivable, negotiable securities, etc., are controlled by a computer, they are vulnerable to fraud and manipulation.

4) loss of data confidentiality- disclosure of personal or proprietary data to unauthorized persons can cause economic loss, dilution of planning efforts, loss of employee morale, and legal action. [Ref. 11]

The potential threats and the losses associated with each threat must be considered together. Each pairing of threat and loss should be ranked according to their impact upon the organization. After this ranking has been developed, the process of examining cost-effective countermeasures can be studied.

This chapter has provided an overview of the nature of the computer security problem today.In particular, the concept of risk assessments has been introduced and its potential benefits to organizations have been considered. The subject of risk assessment and related ideas will be addressed in greater detail in later chapters. Chapter Two will detail the history and evolution of risk assessment requirements within the Department of Defense and the Department of the Navy. Chapter Three will examine various points which must be considered when an organization is deciding whether to do an "in-house" risk assessment or to contract this function with a commercial company. A general framework for conducting a risk assessment at the Naval Postgraduate School will be discussed in Chapter Four.The framework will be based upon the guidelines promulgated in OPNAVINST. 5239.1A. Chapter Five will examine how to design a decision support system to assist management in conducting a risk assessment. Basic design modules will be presented and some particular problems associated with data

base management will be considered. The field of computer security in general, and risk assessments in particular, has advanced to such a degree that several companies now offer automated risk assessment systems. A brief consideration of these systems and a comparison of their attributes vis-a-vis manual systems will also be presented in Chapter Five. The final chapter will summarize the pertinent points covered in this thesis. Some conclusions will be drawn about the state of risk assessments in the modern organizational environment. Lastly, some recommendations to improve the effectiveness and efficiency of the risk assessment process will be presented.

II. DEPARTMENT OF DEFENSE/DEPARTMENT OF THE NAVY DIRECTIVES

A. GENERAL

From the outset, the Federal Government has been a pioneer in the development of advanced computer systems. "The first successful large scale data processing installation was made in the early fifties at the Census Bureau, and the initial impetus toward programming languages for business applications came from Department of Defense support of the COBOL programming language in the sixties" [Ref. 12]. From that point on, the rapid growth of computer technology and the government's reliance on accurate computing systems rose at an exponential rate. Poor accounting and managerial control practices, however, have brought about extreme inaccuracies in the data pertaining to computer hardware and software inventories held by the Federal Government. In 1976, estimates of the amount of money spent on data processing were decidedly vague. "The General Accounting Office (GAO) was able only to bracket Federal Data Processing spending as between $3 billion and $10 billion annually. More recently, the Office of Management and Budget (OMB) has cited a figure of $5.5 billion, and the General Services Administration (GSA) has estimated the cost of software development and maintenance alone at $2.2 billion." [Ref. 12] A large percentage of these expenditures were attributed to the DOD. In 1981, the number of installed computer systems was estimated to be around 15,000, while the number of personnel working in the computer field was estimated at 100,000 [Ref. 12]. These figures, however, are gross approximations.

Since the science of computer technology was a relatively new phenomenon at the time the government began to explore its possibilities, the development of government computer systems was done in a rather piecemeal fashion, with little regard to the managerial aspects of designing and implementing computer systems. The emphasis was on buying/developing and getting the systems into operation as fast as possible in order to show that a functional entity had resulted from all the monetary and personnel resources that had been expended. As a result of this mismanagement (or rather non-management), government agencies were faced with computer systems that were inflexible, inaccurate, and subject to rapid obsclesence. The public outcry over the amount of tax dollars spent on mismanaged computer resources led the Federal Government to issue policy directives addressing computer management from the initiation of requirements analysis to final test and implementation.

B. GOVERNMENT CONCERNS

At about this same time, there was a growing concern over the security vulnerabilities inherent in these new computer systems. Although hardware and software technology had been progressing at a rapid rate, little consideration had been given to computer security technology. However, with the Brooks Act of 1965, the Office of Management and Budget (OMB) had been assigned responsibilities for the oversight and policy-making functions applicable to computer systems development and acquisition. Thus, "in 1972, -- OMB urged private industry -- hardware manufacturers, software houses and related service industries -- to make greater capital investments in computer security. At the time, the Federal Government was concerned that its inability to protect data in computer systems -- except at very great

expense -- was limiting its ability to realize the benefits of technology." [Ref. 13] In December of that same year, the Department of Defense issued DOD Directive 5200.28 entitled "Security Requirements for Automatic Data Processing (ADP) Systems". The purpose of the directive was to establish "uniform policy for protecting classified data stored, processed, or used in, and classified information communicated, displayed, or disseminated by an Automatic Data Processing (ADP) System" [Ref. 14]. Although DOD 5200.28 does not directly address risk assessments, it does require that the heads of DOD components provide for the appointment of an ADP Security Officer, who will later play an important role in conducting risk assessments for Navy computer facilities.[1]

In the mid-1970's, OMB became even more concerned with encouraging the growth of computer security technology since the Privacy Act of 1974 set "forth a series of requirements governing Federal agency personal record-keeping practices" [Ref. 15]. These requirements increased the need to provide security for the personal data maintained in Federal computer systems.

C. LEGISLATION

The Brooks Act also assigned other agencies responsibilities for contributing to the Federal ADP Programs. The National Bureau of Standards (NBS), under the Secretary of Commerce, was tasked with providing "leadership, technical guidance, and coordination of government efforts in the development of guidelines and standards" [Ref. 19]. in

[1] The terms "Risk Analysis" and "Risk Assessment" can be used interchangeably. While early government directives used "Risk Analysis", it is now more common to use "Risk Assessment".

areas pertaining to ADP and ADP Security. The basic philosophy behind the NBS work in ADP Security was reflected in Federal Information Processing Standards Publication (FIPS PUB) 31 of June, 1974: "Data confidentiality and computer security are dependent upon the application of a balanced set of managerial and technological safeguards. Within the context of a total security program, the NBS is pleased to provide guidelines for ADP Physical Security and Risk Management avilable for use by Federal agencies" [Ref. 19].

The concept of Risk Management was introduced at this time to provide federal agencies with guidelines for applying management principles to the risks associated with the acquisition of hardware and software. Although FIPS PUB 31 specifically addresses physical security programs, it also touches upon procedural aspects, contingency planning, supporting utilities, computer reliability, disaster probabilities, security awareness programs, and risk analysis methodolcgies. This publication was one of the first to provide specific recommendations on implementing comprehensive computer security programs. It is important to note, however, that its contents were strictly composed of recommendations and guidelines - they did not constitute a government directive mandating computer security requirements on government agencies. The publication was edited by Susan K. Reed of the Systems and Software Division of NBS. She later authored a government document on conducting risk analyses which would be included as an addendum to DOD 5200.28-M, the Department of Defense ADP Security Manual. This manual will be discussed in more detail in a subsequent section.

It is interesting to note that FIPS PUB 31, published in 1974, covers in great detail those security practices that are advocated by more recent publications. Unfortunately,

the publication has been overshadowed by current directives that dictate what must be done but not how to do it. For example, conventional risk assessments require an analysis of the potential threats to an ADP facility caused by windstorms, hurricanes, and tornadoes. Such information could conceivably be obtained from the National Weather Service, but it is already provided in FIPS PUB 31. In Key West, Florida, to be specific, the annual probability that a hurricane will occur is 13% [Ref. 20]. This figure could be used as direct input to the threat analysis form for the current DOD-advocated risk assessment methodology.

To start a security program, the FIPS encourages all government agencies to "perform a preliminary risk analysis to identify major problem areas and select interim security measures as needed to correct major problem areas" [Ref. 21]. The idea behind this is that, since computer security is an ongoing process, the most obvious security problems should be handled in an expeditious manner - agencies need not and should not wait until a comprehensive risk assessment has been completed prior to tackling the serious security problems. In the meantime, a preliminary assessment should be done to help isolate those problems.

The actual risk assessment methodology presented in the FIPS is a sound one. It gives an excellent overview of the means by which a risk assessment may be conducted, complete with charts, tables, and figures that the user may apply in calculating the final Annual Loss Expectancy (ALE) value. However, the publication is somewhat weak when it comes to describing the format or layout of an agency's actual risk assessment document.

D. DEFINITIONS

Before going into the specific risk assessment methodology outlined in the FIPS, it is appropriate to define certain terms which are common to most, if not all, government-endorsed risk assessment methodologies :

THREAT -an overt or covert activity which may cause loss or damage to a computer facility;

LOSS -the potential for being deprived of computer assets or services;

VULNERABILITY -the weakness inherent in a computer system, which makes it susceptible to loss or damage;

ANNUAL LOSS EXPECTANCY (ALE) -an estimate of the amount of money that a computer facility could potentially lose in a year if threats against the facility were realized.

E. FIPS PUB 31 METHODOLOGY

The FIPS methodolgy is basically a three-step process : 1.) Make an estimate of the potential losses to which the computer facility is exposed; 2.) Perform an analysis of the threats which may be made against the facility; and 3.) Combine the estimates of potential loss and probability of loss to produce an ALE value.

1. Estimating Loss

Step one, estimates of potential losses, is to be done in terms of five distinct categories : "(1) physical destruction or theft of physical assets; (2) loss or destruction of data and program files; (3) theft of information; (4) theft of indirect assets; and (5) delay or prevention of computer processing" [Ref. 21]. The end products of

this procedure are an identification of the computer facility's assets and dollar values for loss estimates.

Of the five categories listed, the first is undoubtedly the most straightforward. Replacement costs for such items as hardware, communications equipment, supplies, and the building itself should be entered into the command's inventory files as required by GSA. Unfortunately, many federal agencies have neglected to maintain inventory files over the years. One of the fringe benefits of a risk assessment is that such inventories must be generated, thus enhancing a command's resource management capabilities. Once these inventories have been made available, the estimate of loss for a particular piece of equipment corresponds to its replacement cost. For example, if a high-speed line printer costs $5000, then its loss estimate would be the same - the command has the potential for losing $5000 if the printer were to be destroyed or stolen.

In the second and third categories, loss or destruction of data and program files and theft of information, a great deal of ambiguity occurs. The question which must be answered is : What is the value of the data contained in the computer system ? This is a question which has received a great deal of attention in recent years. The Commander, Naval Data Automation Command (COMNAVDAC), spent a significant amount of time and money in trying to bring the question of the value of data into perspective. Some consideration was given to standardizing data value based on the number of lines of code and/or security classification. A single line of code in a 100-line program file might be valued at $10, for example. The loss or destruction of the file would thus contribute $1000 to the agency's ALE. In essence, it would cost the command $1000 to reconstruct the file. In a similar manner, a word of SECRET or TOP SECRET

code, if compromised or stolen, might be valued at $100 and $200 respectively. By standardizing these values, computing the ALE for most types of computer software would be a simple matter of mathematical calculation, with lines of code (the amount of money it would cost a programmer to reproduce the code) being an absolute value, and classified code representing a relative value. In theory, such methods have a sound basis. In practice, however, the application of such methods has proven to be rather unrealistic. In fact, COMNAVDAC has recently abandoned its attempts to provide for standardization in favor of more practical methods.

"If the ADP system is used to control other assets such as cash, items in inventory, or authorization for performance of services, then it may also be used to steal such assets." [Ref. 22]. These assets are known as indirect assets, and their loss estimate corresponds to the real value of the asset.

In estimating the potential loss caused by the delay or prevention of computer processing, several considerations must be addressed. Some losses may be estimated in a relatively straightforward manner. Obvious examples involve a failure to process payment checks promptly, thereby preventing the exercise of a prompt payment discount under a procurement contract, or delays in an inventory system which may lead to idle manpower at a warehouse [Ref. 22]. In a situation where a computer facility functions as a service agency, the loss estimate would be based on the revenues lost as a result of the customers being denied access to the computer system. On the other hand, "...in those situations where a delay would more or less halt operations of an agency,...use the daily operating cost of an agency as a rough rule-of-thumb estimate of the cost of delayed processing" [Ref. 22].

In general, there are time ranges or limits within which loss estimates will differ. If service is denied but the system can be brought back up within a reasonable amount of time, it is possible that no loss will be incurred during that time period. However, after a certain period of time during which the computer system has not been returned to service, losses will be incurred, and in general, such losses will grow in proportion to the duration of the delay. The FIPS PUB stresses the importance of establishing this "maximum 'no loss' delay time and an estimate of the median time to reconstruct the ADP facility after total destruction" [Ref. 22]. Once these time/cost boundaries have been made, then the time period can be divided into various ranges and loss estimates can be assigned accordingly.

TABLE I
Loss Exposure

Task	Loss of Data	Theft of Info.	Theft of Assets	Delayed Processing
Q	Yes	No	No	Extreme
R	Yes	Yes	Yes	Moderate
P	No	Yes	Yes	Moderate
T	No	Yes	Yes	Low
S	No	No	No	Very Low

After conducting a preliminary estimate of all potential losses, the task might be simplified by presenting the collected data in tabular form, as shown in Table I extracted from FIPS PUB 31.

TABLE II

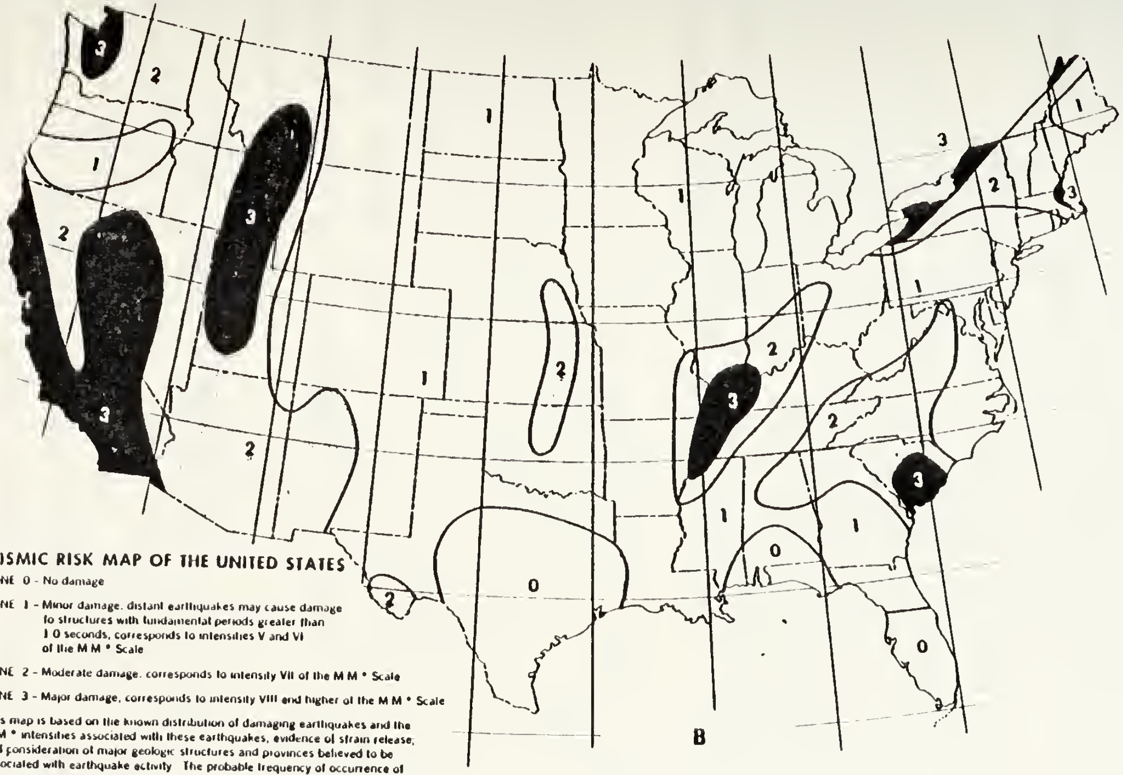
Sources for Threat Information

Threat	Sources of Information
Fire	Building fire marshal and local fire department
Flood	Army Corps of Engineers
Earthquake	National Earthquake Information Center
Windstorm	National Oceanic and Atmospheric Administration and local National Weather Service Office
Power Failure	Building Engineer and local public utility
Air Conditioning Failure	Building Engineer and air conditioning vendor
Communications Failure	Federal Telecommunications System, building and local telephone company
ADP Hardware Failure	Hardware vendors and Federal Supply Service
Intruders, Vandals,etc.	Building manager, security director and the Office of Federal Protective Service Management, GSA.
Compromising Emanations	Hardware vendors and the Office of Federal Protective Service Management, GSA.
Internal Theft or Misuse	System Design, Internal Audit and Personnel Division

2. Evaluating Threats

In proceeding with the second step of the risk assessment, that of evaluating the threats against the ADP facility, the ADP Security Planner (ie. the person responsible for conducting the overall risk assessment) should solicit the help of fire marshals, hardware vendors, other government agencies, in house personnel, and/or any agency or person who might contribute inputs to a threat evaluation. Table II provides a list of sources of information for different categories of threats.

Although the FIPS gives little information on the specific numerical figures to use in quantifying threats, it does provide specific guidance on determining threat probabilities. Figure 2.1, for example, a seismic risk map of the United States, gives the user a rough idea of the long-term hazards caused by earthquakes.



SEISMIC RISK MAP OF THE UNITED STATES

ZONE 0 - No damage

ZONE 1 - Minor damage. distant earthquakes may cause damage to structures with fundamental periods greater than 1 0 seconds, corresponds to intensities V and VI of the M M * Scale

ZONE 2 - Moderate damage. corresponds to intensity VII of the M M * Scale

ZONE 3 - Major damage, corresponds to intensity VIII and higher of the M M * Scale

This map is based on the known distribution of damaging earthquakes and the M M * intensities associated with these earthquakes, evidence of strain release, and consideration of major geologic structures and provinces believed to be associated with earthquake activity The probable frequency of occurrence of damaging earthquakes in each zone was not considered in assigning ratings to the various zones

*Modified Mercalli Intensity Scale of 1931

Seismic risk maps. Because of the relatively short recorded history of seismic events in the United States, such maps can give only a rough idea of the long-term hazard The maps are based on the actual occurrence of earthquakes and major geologic structures and provinces, but do not consider local physical conditions. No common time-scale is implied; actually, major earthquake damage would not be expected to occur as frequently in an East Coast Zone 3 as in a West Coast Zone 3. (A) Map compiled in 1948-1952, and incorporated into many building codes and regulations The dots represent past occurrences of damaging earthquakes, and are defined as follows: smallest dots, negligible damage to buildings of good design; next smallest, slight damage to buildings of good design; second largest, considerable damage to buildings of good design; largest dots, great damage, fissures, visible vertical and horizontal ground movements (B) Map released in 1969, based on additional seismic studies. (ESSA/USC&GS)

Figure 2.1 Seismic Risk Map.

3. Calculating the Annual Loss Expectancy (ALE)

The final step in the risk assessment process itself, although follow-on action is understood, involves the determination of the ALE. This can be accomplished (and most readily understood) by constructing a matrix of threats and the losses which might be associated with them. Table III shows a computation for estimating the expected losses that might be caused by fire damage.

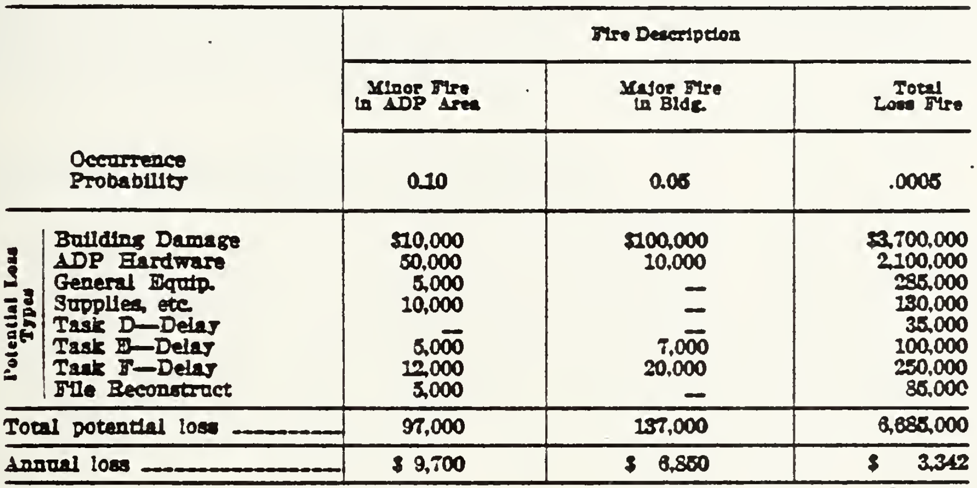
Construction of such a table is a common procedure in operations research and management sciences where the objective may be to minimize losses (as in this case) or maximize profits. The occurrence probabilities shown (.10, .05,.005) may be derived by analyzing the facility's fire safety precautions, a procedure for which the FIPS PUB gives detailed guidance.

The dollar amounts for loss may be computed as described earlier in the chapter. Once these figures have been made available, estimates for the total potential loss and the annual loss for each category can be calculated by multiplying the occurrence probability by the loss figures. Similar tables can be constructed for natural disasters such as earthquakes, tornadoes, volcanic eruptions, floods, and others.

Upon completion of the estimation of the ALE for all categories of loss, the security manager should have a clearer understanding of the coupling of threats and losses within his facility. He is then in a position to prioritize his work in the area of computer security countermeasures. In general, remedial measures should be applied to those areas in which the loss potential is the greatest. The end result, then, of the risk assessment process is a cost-benefit analysis of expending funds towards the "securing"

TABLE III

Estimating Fire Loss



		Fire Description		
		Minor Fire in ADP Area	Major Fire in Bldg.	Total Loss Fire
	Occurrence Probability	0.10	0.05	.0005
Potential Loss Types	Building Damage	$10,000	$100,000	$3,700,000
	ADP Hardware	50,000	10,000	2,100,000
	General Equip.	5,000	—	285,000
	Supplies, etc.	10,000	—	130,000
	Task D—Delay	—	—	35,000
	Task E—Delay	5,000	7,000	100,000
	Task F—Delay	12,000	20,000	250,000
	File Reconstruct	5,000	—	85,000
Total potential loss		97,000	137,000	6,685,000
Annual loss		$ 9,700	$ 6,850	$ 3,342

of a specific computer security weakness. If, for example, the ALE for building damage caused by fire is $ 9,700 , the agency should be willing to spend up to that amount in providing remedial measures to lessen that loss potential. The risk assessment will thus provide the security manager with the ammunition he needs to get top management support on funds for security countermeasures.

The preceding synopsis of the FIPS methodology might seem to be, as presented, a relatively straightforward process. However, the FIPS PUB clearly states, "...this is not an exact science. Indeed, it is quite likely that one will have to reappraise threats and losses more than once, concentrating on the areas initially identified as most

critical, before the loss expectancy estimate reaches a satisfactory level of confidence." [Ref. 23]

The level of detail provided for the above FIPS PUB methodology will serve as a point of reference for descriptions of subsequent methodologies. Other risk assessment methodolcgies will be discussed in terms of how they differ from the one described in FIPS PUB 31.

F. SUBSEQUENT GOVERNMENT DIRECTIVES

Shortly after the release of FIPS PUB 31, the Privacy Act of 1974 was enacted. OMB Circular A-108, distributed six months later, was written to assign responsibilities for the security of the personal records maintained by Federal agencies. Under this directive, the term "system of records" was defined as "...a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual" [Ref. 16]. Since computer and word processing systems are perfect vehicles for data storage and retrieval, it was and is only natural that they would be used for the maintenance of personal records. A-108 further mandated that reasonable administrative, technical, and physical safeguards are established to ensure that personal records are only disclosed to those who are authorized to have access to them [Ref. 17]. This implies that security countermeasures must be in effect for all federally-owned computer systems maintaining personal data. The directive also required that the GSA "revise computer and telecommunications procurement policies to provide that agencies must review all proposed equipment and services procurements to assure compliance with applicable provisions of the Act" [Ref. 18]. This was the first of many government directives

requiring that federal agencies address security issues in their computer development and acquisition plans. However, outside of FIPS PUB 31, the distribution and knowledge of which was very limited, the Federal Government was slow to document specific policies and procedures for implementing computer security programs.

Finally, three years later in July, 1978, OMB Circular A-71, entitled "Security of Federal Automated Information Systems", was approved for distribution. In general, the purpose of A-71 was to promulgate "policy and responsibilities for the development and implementation of computer security programs by executive branch departments and agencies" [Ref. 24]. This circular documented the requirement that periodic risk assessments be conducted by each federal agency operating a computer facility. Although A-71 provided no guidelines on how to conduct a risk assessment, it did require that a risk assessment be carried out or revised under any of the following conditions :

1.) prior to the approval of design specifications for new computer installations;

2.) whenever there is a major change to the physical facility, hardware or software; or

3.) at periodic intervals of time, not exceeding five years, if no risk assessment has been performed during that time.

[Ref. 25]

This directive had serious consequences for all federal agencies. For most agencies, the third condition was the one under which the risk assessments would be conducted. Those agencies which had yet to perform a risk assessment

interpreted the condition as meaning that they had a five-year deadline on the requirement. Unfortunately, this slowed response from many federal agencies.

To promulgate the requirements of A-71, the Department of the Navy issued OPNAVINST 5239.1 in April, 1979. This instruction specified the A-71 requirements for all DON activities. Although the instruction did little to augment the policies provided by A-71, it did require that all DON activities operating computer installations appoint an ADP Security Officer who would be responsible for ensuring that a risk assessment would be conducted on a periodic basis. Two relevant enclosures that were included as part of OPNAVINST 5239.1 were DOD 5200.28-M entitled "Techniques and Procedures for Implementing, Deactivating, Testing, and Evaluating Secure Resource-Sharing ADP Systems", and a set of guidelines for conducting risk assessments which was edited by Susan K. Reed. The former, constituting the DOD ADP Security Manual, provided standardized guidelines for securing computer systems - it did not address risk assessments; the latter, however, provided an excellent generic framework for conducting risk assessments. It's merit was more in facilitating the security officer's understanding of the risk assessment model than in the actual methodolgy proposed. The technique presented by the methodology is similar to that presented in FIPS PUB 31, but is a more mathematically-oriented model. These guidelines were later released in August, 1979, as FIPS PUB 65, "Guideline for Automated Data Processing Risk Analysis".

G. FIPS PUB 65 METHODOLOGY

In general, FIPS PUB 65 "explains the reasons for performing a risk analysis, details the management involvement necessary and presents procedures and forms to be used

for risk analysis and cost effective evaluation of safeguards" [Ref. 26]. Unlike FIPS PUB 31, this NBS publication gives no guidance on estimating specific loss probabilities (ie. there are no seismic risk maps or tables with hurricane probabilities for various regions), but it does provide a better and more detailed explanation of the quantitative measures and forms required for a risk assessment. In short, FIPS PUB 65 covers the ambiguities present in FIPS PUB 31. The two in combination provide a powerful framework under which a viable risk assessment can be conducted.

Like most methodolcgies, the one advocated by FIPS PUB 65 recommends that a preliminary security analysis be performed in order to identify a computer installation's assets, threats, vulnerabilities, and thus, the facility's security posture. Three specific products will result from this preliminary analysis :

1.) a list of asset replacement costs;

2.) a list of threats to which the facility is vulnerable; and

3.) a list of existing security measures. [Ref. 27]

These products, once assigned quantitative measures, will form the basis for the computation of the ALE(s).

The next step in the FIPS methodology is to quantify the measures for impact and the frequency of occurrence for threats. The impact of an event is defined as the exact amount of damage it could cause, while the frequency of occurrence refers to the exact number of times the event could occur. [Ref. 28] The common denominator selected for the measures is monetary value, and a year is the time period against which frequencies of occurrence will be assessed. To simplify such quantitative measures, estimates

for impact and frequency are rounded off to factors of ten. The range of measures for both categories is shown in Table IV.

TABLE IV

Orders of Magnitude of Estimated Impact and Frequency

IMPACT:

$10
$100
$1000
$10,000
$100,000
$1,000,000
$10,000,000
$100,000,000

FREQUENCY:

Once in 300 years
Once in 30 years
Once in 3 years (1000 days)
Once in 100 days
Once in 10 days
Once per day
10 times per day
100 times per day

The FIPS emphasizes that rounding off the figures will not have a significant effect on the overall ALE. The relevance lies in orders of magnitude rather than in absolute figures. Thus, "there will be no significant difference in the overall exposure whether the damage from a certain event is estimated at $110,000 or $145,000...(or)...if the frequency of an event is expected to be twelve times a year or thirty" [Ref. 29]. Once the impact and frequency measures have been determined, the ALE can be readily calculated using the following formula :

LOSS = IMPACT(I) x FREQUENCY OF OCCURRENCE (F)

To use this formula, however, it is first necessary to index the impact (i) and the frequency (f) measures from Table IV. The resulting indices are shown in Table V.

TABLE V

Table for Selecting of Values of i and f

If the estimated cost impact of the event is

$10,	let i = 1
$100,	let i = 2
$1000,	let i = 3
$10,000,	let i = 4
$100,000,	let i = 5
$1,000,000,	let i = 6
$10,000,000,	let i = 7
$100,000,000,	let i = 8

If the estimated frequency of occurrence is

Once in 300 years,	let f = 1
Once in 30 years,	let f = 2
Once in 3 years,	let f = 3
Once in 100 days,	let f = 4
Once in 10 days,	let f = 5
Once per day,	let f = 6
10 times per day,	let f = 7
100 times per day,	let f = 8

To use the indices in the previous equation, they must first be related to Impact (I) and Frequency of Occurrence (F). Such relationships are expressed in the following equations :

for Impact, $I = 10^{i}$

for Frequency, $F = 10^{(f-3)}/3 = 10^{f}/3000$

Thus, if the impact of an event is estimated at $100 (i=2 from Table V) then $I = 10^i = 10^2 = 100$. Similarly, if the frequency of occurrence is estimated to be once per day (f=6), then $F = 10^f/3000 = 10^6/3000 = 333.3$.

Consider the following practical example, where the potential impact of a hurricane is $100,000 in damage to a computer facility, and the frequency for a hurricane is once in thirty years. The ALE would then be computed as follows :

IMPACT : $100,000 (i=5)

$I = 10^5 = 100,000$

FREQUENCY : 1/30 years (f=2)

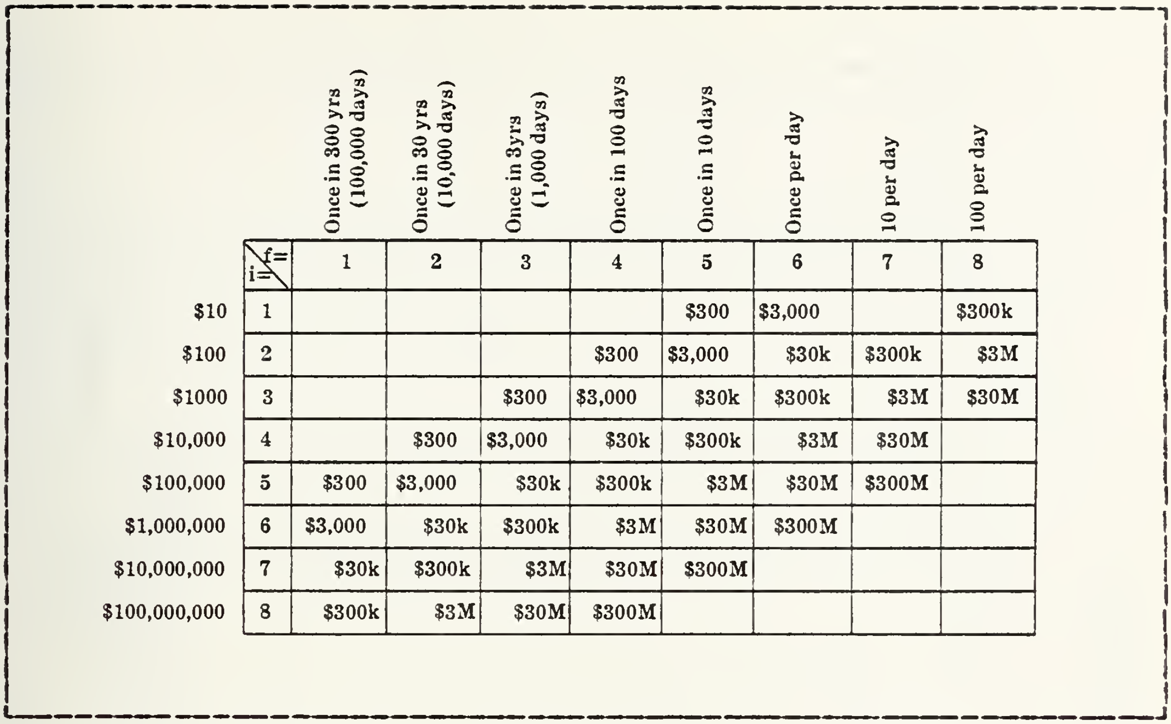
$F = 10^2/3000 = .0333$

LOSS: $I \times F = 100,000 \times .0333 = 3,330$

Thus, the ALE resulting from a hurricane would be approximately $3,000.

It is not necessary, howvever, to compute the ALE using these tedious and cumbersome equations. The FIPS PUB provides figure 2.2 to facilitate the process. The ALE for a particular event can then be found at the intersection of the values estimated for impact and frequency.

When all ALEs have been calculated, the FIPS PUB suggests that the approach to the remainder of the task be done in an orderly and structured manner. In short, it recommends that "...the risk analysis task is better approached from the standpoint of the data files, or applications systems, of which there is a finite number" [Ref. 30].

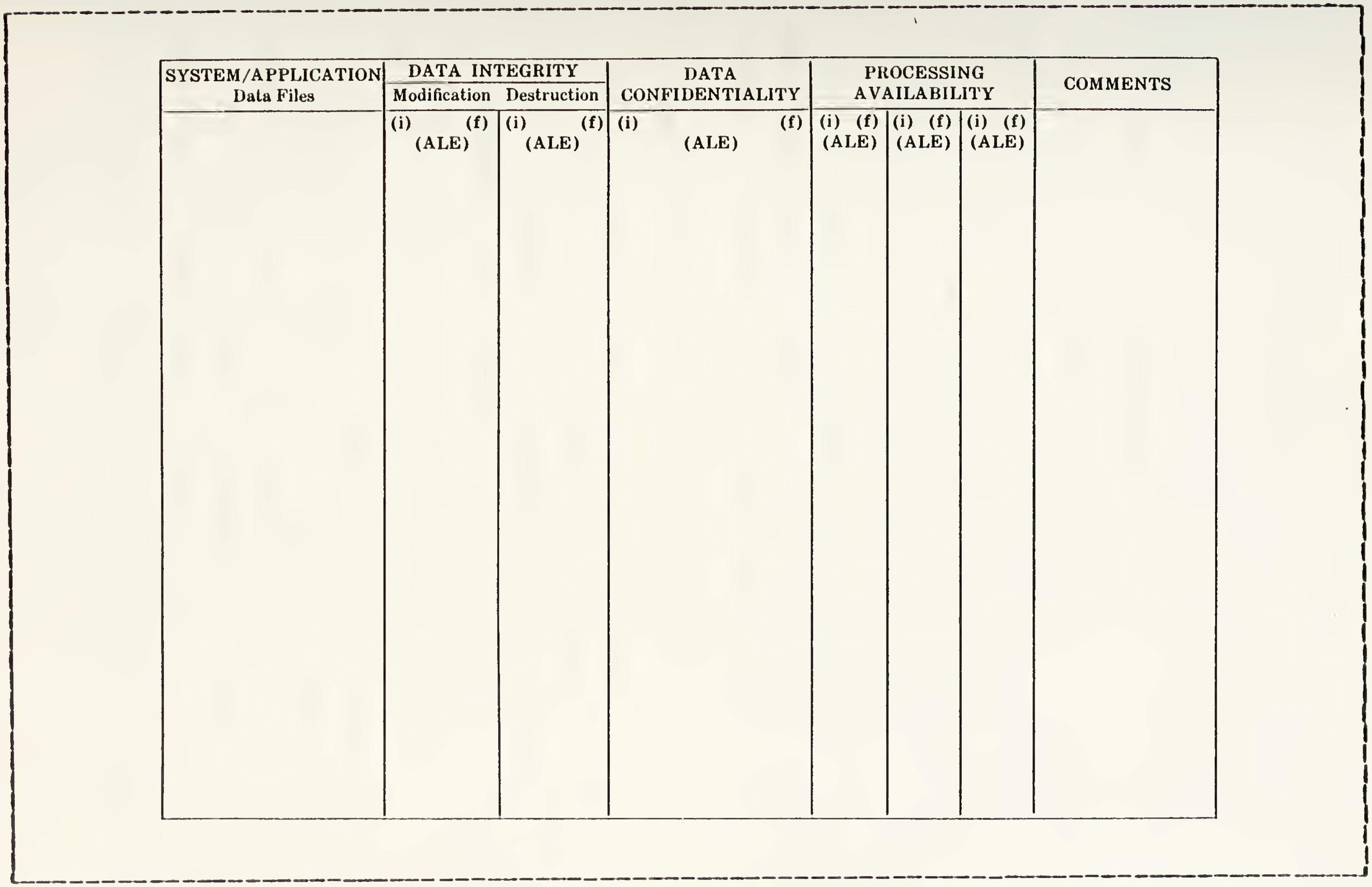


		Once in 300 yrs (100,000 days)	Once in 30 yrs (10,000 days)	Once in 3yrs (1,000 days)	Once in 100 days	Once in 10 days	Once per day	10 per day	100 per day
	i= \ f=	1	2	3	4	5	6	7	8
$10	1					$300	$3,000		$300k
$100	2				$300	$3,000	$30k	$300k	$3M
$1000	3			$300	$3,000	$30k	$300k	$3M	$30M
$10,000	4		$300	$3,000	$30k	$300k	$3M	$30M	
$100,000	5	$300	$3,000	$30k	$300k	$3M	$30M	$300M	
$1,000,000	6	$3,000	$30k	$300k	$3M	$30M	$300M		
$10,000,000	7	$30k	$300k	$3M	$30M	$300M			
$100,000,000	8	$300k	$3M	$30M	$300M				

Figure 2.2 Combined Matrix of i, f, and ALE.

In terms of such software considerations, the publication discusses three conditions which might result if a threat to a computer system were realized : DATA INTEGRITY (eg. destruction or unauthorized modifications to data); DATA CONFIDENTIALITY (ie. a compromise of classified data); and ADP AVAILABILITY (pertaining to the amount of time that a computer system can be returned to service after failure).

To provide structure and order to the recording of the risk assessment findings, the FIPS PUB supplies the worksheet presented as figure 2.3 Such a worksheet might simplify the record-keeping aspect of the process, but it is only a suggestion - if used, it should be formatted or tailored to an agency's needs.



SYSTEM/APPLICATION Data Files	DATA INTEGRITY		DATA CONFIDENTIALITY	PROCESSING AVAILABILITY			COMMENTS
	Modification	Destruction					
	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	

Figure 2.3 FIPS PUB 65 WORKSHEET.

On this particular worksheet, data files are listed separately, and arranged by application. Impact and frequency estimates and ALE(s) for each category of threat are then listed alongside the associated file. A comments column is provided to allow for an amplification of the figures shown. As an additional guide to using these work sheets, the FIPS PUB presents a practical example (for a small organization) of a complete risk assessment.

The FIPS PUB attempt to structure the risk assessment process adds a degree of credibility to the overall methodology. However, it is unreasonable to expect that the whole process can be carried out as a "cookbook" method. There are definite limits to structuring such a task, particularly in areas such as identifying and estimating the threats against a facility. In short, "ADP risk analysis is a technique which relies heavily on the intuition, experience and technical knowledge of the team members" [Ref. 30].

H. CURRENT DIRECTIVES

Approximately a year after the release of FIPS PUB 65, the NBS distributed a ten-page document entitled "Risk Analysis Standard". The purpose of this document was simply to standardize the terminology and concepts behind the DOD philosophy for conducting risk assessments. It did not supply any specific guidelines or methodologies.

Finally, in August, 1982, the DON approved and distributed OPNAVINST 5239.1A, a full and comprehensive manual describing the Navy's ADP Security program. A significant portion of this manual addresses the approved DON risk assessment methodology, complete with forms and specific directions. The procedural aspects of this methodology will be presented as a practical framework for a risk assessment

that could be conducted at the Naval Postgraduate School. in Chapter 4.

This chapter has described how the currently-approved DON methodology has evolved over the years. Figure 2.4 shows a time line of the events leading up to the distribution of OPNAVINST 5239.1A.

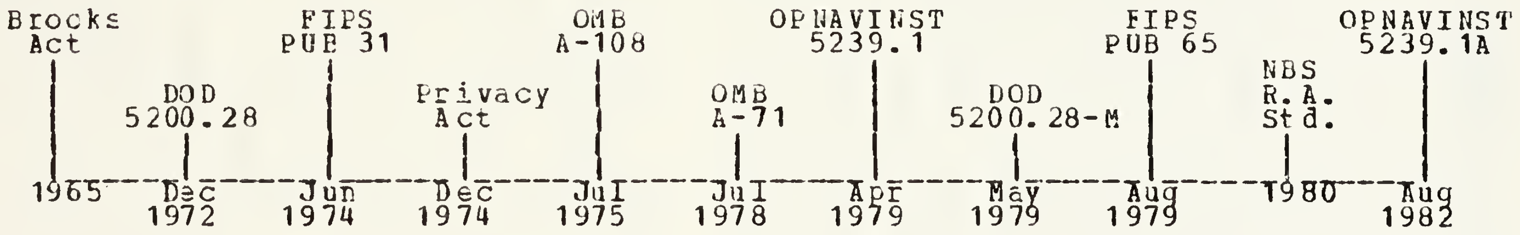


Figure 2.4 Time Line of Government Directives.

III. IN-HOUSE VS CONTRACTUAL SUPPORT

A. GENERAL

With the distribution of OMB Circular A-71 in 1978 came the requirement that a "Risk Assessment" (sometimes referred to as a "Risk Analysis") be conducted at each computer installation operated by a federal agency. While the risk assessment methodology currently recognized within the Department of Defense is a manual system, there are commercial software packages available, notably PANAUDIT by Pansophic Systems, which could facilitate the "number-crunching" aspect of risk assessments. Unfortunately, this particular software is only IBM-compatible, and thus has limited application to Navy computer systems.

In the past few years, numerous government directives and guidelines on methodologies for conducting risk assessments have been disseminated. Many of these have resulted from a joint effort on the part of government and commercial industry. In 1977, in an effort to perfect a more concise methodology that could be applied to various sizes and types of computer systems within the Department of the Navy, COMNAVDAC let a contract with Systems Development Corporation (SDC) to develop and document such a methodology. This contract, involving contractor support services, falls under the Policy/Program Review category outlined in NAVMATINST 4200.50C. The justification for contracting out such a service was undoubtedly a matter of the expertise held by the commercial marketplace. The

result of the contract with SDC is contained in NAVDACINST 5510.1, the Department of the Navy ADP Security Manual. While still in draft form, the distribution of this manual will serve as an excellent reference for those Naval agencies about to initiate a risk assessment.

1. The Need for Contractual Support

Many government directives pertaining to ADP Security provide guidance on the in-house personnel an agency must use to form their risk assessment team. Such personnel generally include representatives from ADP Operations Management, Systems and Applications Programming, Hardware Maintenance, Communications Engineering, Internal Auditing, and the Security Staff. Since a comprehensive risk assessment is a time-consuming process, diverting the services of these individuals from their normal duties could well create a hardship within their divisions or departments. This potential hardship was recognized by personnel at NAVDAC who began to consider the possibilities of allowing for contractual support in conducting risk assessments. Although previous directives only discussed conducting risk assessments in terms of using in-house personnel resources, NAVDACINST 5510.1 mentions that qualified contractors may be used with prior approval from NAVDAC.

2. A Prototype for a Contracted Risk Assessment

In early 1980, personnel at the Fleet Numerical Oceanography Center (FNOC) in Monterey, California, began to have serious doubts about their ability to conduct an in-house risk assessment. The computer configuration at FNOC, consisting of numerous large-scale mainframes, communications networks and devices, minicomputers, and peripherals, was extremely large and complex. It would be very

difficult to spare the key personnel needed on the risk assessment team from their everyday duties. With this in mind, the ADP Security Officer at FNOC wrote to NAVDAC asking for guidance on using contractor assistance. NAVDAC, which had been giving this issue a great deal of thought, decided to use FNOC as a prototype for future contracted risk assessment efforts. To this end, NAVDAC offered to lend technical assistance, provide liaison with the contractor and other knowledgable government agencies, and oversee the entire process. The government agencies to be involved (directly or indirectly) in the process are those shown in figure 3.1, which was extracted from NAVDACINST 5510.1X [Ref. 33]. These agencies roughly parallel those which play a key role in federal acquisition policies and procedures.

3. Standardization in Contracted Risk Assessments

While the end result of this contract effort was to be a completed risk assessment, it was also serving as a standard against which future risk assessments could be conducted. Thus, as concerns arose during the project, NAVDAC documented them and considered ways in which the process could be enhanced and standardized. This study will briefly summarize the events that occurred during FNOC's risk assessment, show how NAVDAC monitored and controlled the whole process, and describe how NAVDAC has streamlined the system to facilitate contractor support on any activity's risk assessment.

4. Preliminary Efforts

NAVDAC's first priority in assisting FNOC was to gather a pool of personnel whose technical expertise would facilitate the project. To this end, FNOC was provided a copy of NAVDACINST 5230.1A, "Procedures for Requesting

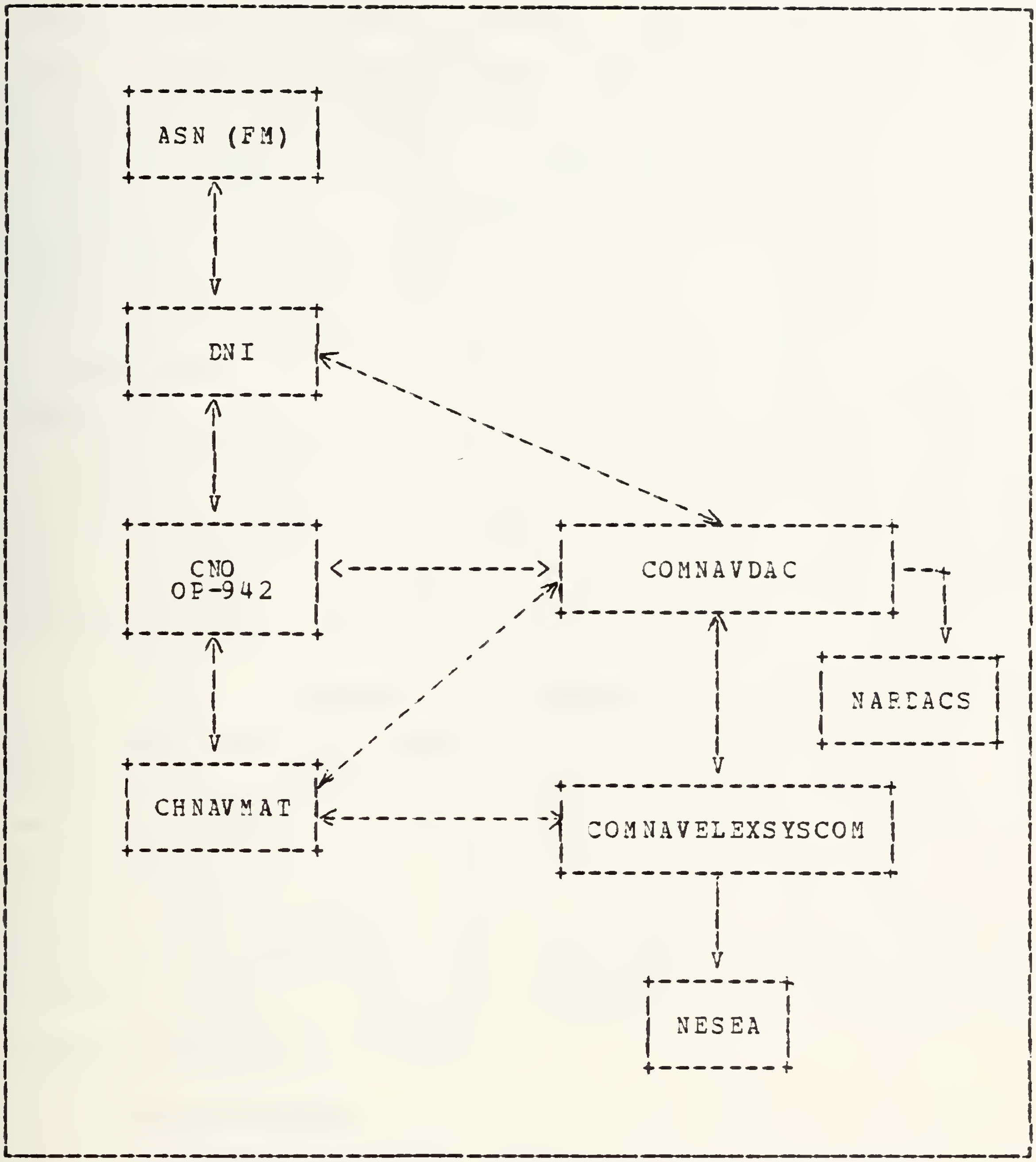


Figure 3.1 DON/ADP security Organizational Relationships.

Services from Navy Regional Data Automation Centers (NARDACs)". FNOC's task was to generate a letter requesting technical support services from NARDAC, San Francisco. Included in this letter was information pertaining to

project title, requesting command, type of request, objectives, security classification, and funding. Identifying the source of the funding is an important consideration in requesting NARDAC services. "Commencing in fiscal year 1982 all Navy customers of a NARDAC, except Navy industrial Fund Activities, will be supported on an entirely mission funded basis...Unprogrammed costs which cannot be accommodated will be subject of discussion between the NARDAC and the customer to determine if other means of funding are available" [Ref. 34]. In this situation, FNOC had budgeted $100K for the risk assessment project, and the NARDAC had no funds available. It was thus determined that FNOC would remit the $100K to the NARDAC, who along with NAVDAC, would use the funds to cover the costs of the government's technical support personnel and the contractor's fees.

Once the method of funding had been determined, NAVDAC sent technical experts from the NARDAC, NAVELEX, and NESEA (Naval Electronics Systems Engineering Activity) to FNOC to discuss the program with ADP Security personnel. These personnel outlined the project and generated a document on FNOC's computer assets for use by the contractor. NAVDAC, in the meantime, was using inputs from this group to generate a plan of action and milestones that the contractor would be expected to follow.

5. The Contract

NAVDAC handled all the requirements for negotiating and awarding the contract. The details, however, on the negotiations, evaluation, selection, and award were not available to the authors. After the negotiations had been completed, the contract was awarded to Systems Development Corporation (SDC).

By the time the SDC personnel arrived at FNOC, they had been in constant touch with the project manger at NAVDAC, and were well aware of the tasks expected of them. By interviewing personnel from all areas of FNOC's organizational components, reviewing computer configuration schematics and documentation, penetrating computer security vulnerabilities and merging them with potential threats, they were able to assess FNOC's security posture and produce the required documentation and Annual Loss Expectancy (ALE) figures.

6. Future Risk Assessment Contracts

Since a risk assessment contract will call for a study or analysis of the security aspects of an existing computer system, it will have to adhere to the requirements of NAVMATINST 4200.50C which addresses contractor support services. If FNOC's contract was any indication, future risk assessment contracts will undoubtedly exceed $50k, and thus will require legal review and approval by "...a level no lower than Flag or General Officer or individuals in the Senior Executive Service (SES)" [Ref. 31].

In an effort to make FNOC and its parent command, Commander, Naval Oceanography Command (CNOC), more autonomous in contracting for future ADP security-related services, NAVDAC recently drafted a letter in which the subject line reads, "Automated Data Processing (ADP) Security Accreditation and Contractor Assistance". This document will be invaluable to any Naval activity considering contract support in completing a risk assessment. Although the information will not be afforded general distribution, NAVDAC is amenable to providing it when requested by a Navy activity. The several enclosures to the document constitute sample ADP security contracting docu-

ments, which as NAVDAC mentions, must be tailored to specific tasking requirements and coordinated with the local Navy Regional Contracting Center. NAVDAC's purpose in this effort is "...an attempt to assure that Navy activities receive quality contractor ADP security reports and products for dollars invested" [Ref. 32].

Among the enclosures is a sample statement of work which may be tailored and included as part of an activity's Request for Proposal (RFP), or in NAVDAC terms, Task Order or Task Request. The sample not only addresses risk assessments, but also includes other ADP security areas which may be candidates for contractor assistance : Risk Assessment Planning, Contingency Plan Testing, and Security Training. It is the job of an activity's ADP Security Officer to write a task request based on the statement of work, describing the specific area of the work required. NAVDAC's sample work statement has specific guidelines on the necessary wording, including a list of military publications to which the contractor must be responsive, and a list of required deliverables such as summary progress reports, schedule of performance, and contract financial progress reports. The sample work statement also includes an option to extend the term of the statement of work. This will be renewable at prices stated by the contractor and at the option of the government. In addition, NAVDAC provides guidance on the Government-Furnished Equipment and documentation that an activity should be prepared to provide the contractor. Other documents NAVDAC has included as samples are : the Contract Security Classification Specification, detailing the security considerations and access requirements; Contractor Personnel Qualifications Statement, describing the minimum qualifications expected of the contractor personnel assigned to the project; Personal vs Nonpersonal

Services Questionnaire, a document used by the contracting officer to determine whether or not the solicited service is nonpersonal; and the Contract Data Requirements List, which describes the required deliverables. These are all standard requirements for an RFP, but they have been uniquely tailored for a Risk Assessment application.

As of 28 July 1982, NAVDAC had approved six organizations to be included on the Bidder's Mailing List. These organizations and their qualifications are shown in figure 3.2. At the time of this writing, three were qualified to conduct risk assessments, but only two of these had DON approval. Two of the organizations listed were small businesses.

Each of these vendors will be notified of a task request by the Contract Administration Office (CAO). Vendors are required to pick up the task request within a week of notification. NAVDAC refers to vendor responses as "Task Order Proposals" (TOPs). As is the case with standard RFPs, these are due at a specified time and date.

DON ADP Security Contractor Qualifications Matrix
28 July 1982

Corporation*	Applied for DON Approval	DON Approval	Small Business	8A	Large Business	Type work: Gen.Sec.	Risk	ST&E
ADP Graphics	-	-	-	-	X	X	-	-
CISI	-	-	-	-	X	X	-	-
EDP Auditors	-	-	-	-	X	X	-	-
Info Systems, Inc.	X	-	X	X	-	X	X	X
AA Audit Co.	X	X	X	X	-	X	X	-
ZZ Consulting	-	X	-	-	X	X	X	X

*The corporations listed above are fictitious. The names and information in this matrix have been modified in the interest of protecting proprietary data.

Figure 3.2 Small Business Matrix.

7. Proposal Evaluations and Selection

Information required in a TOP for a risk assessment includes "the number of man-hours by skill category by task and subtask, milestone dates, travel costs, proposed pricing arrangements, personnel resumes, and technical approach" [Ref. 32]. The function of the activity's technical evaluation board, chaired by the ADP Security Officer, who is generally assigned as project manager, will be to evaluate these factors.

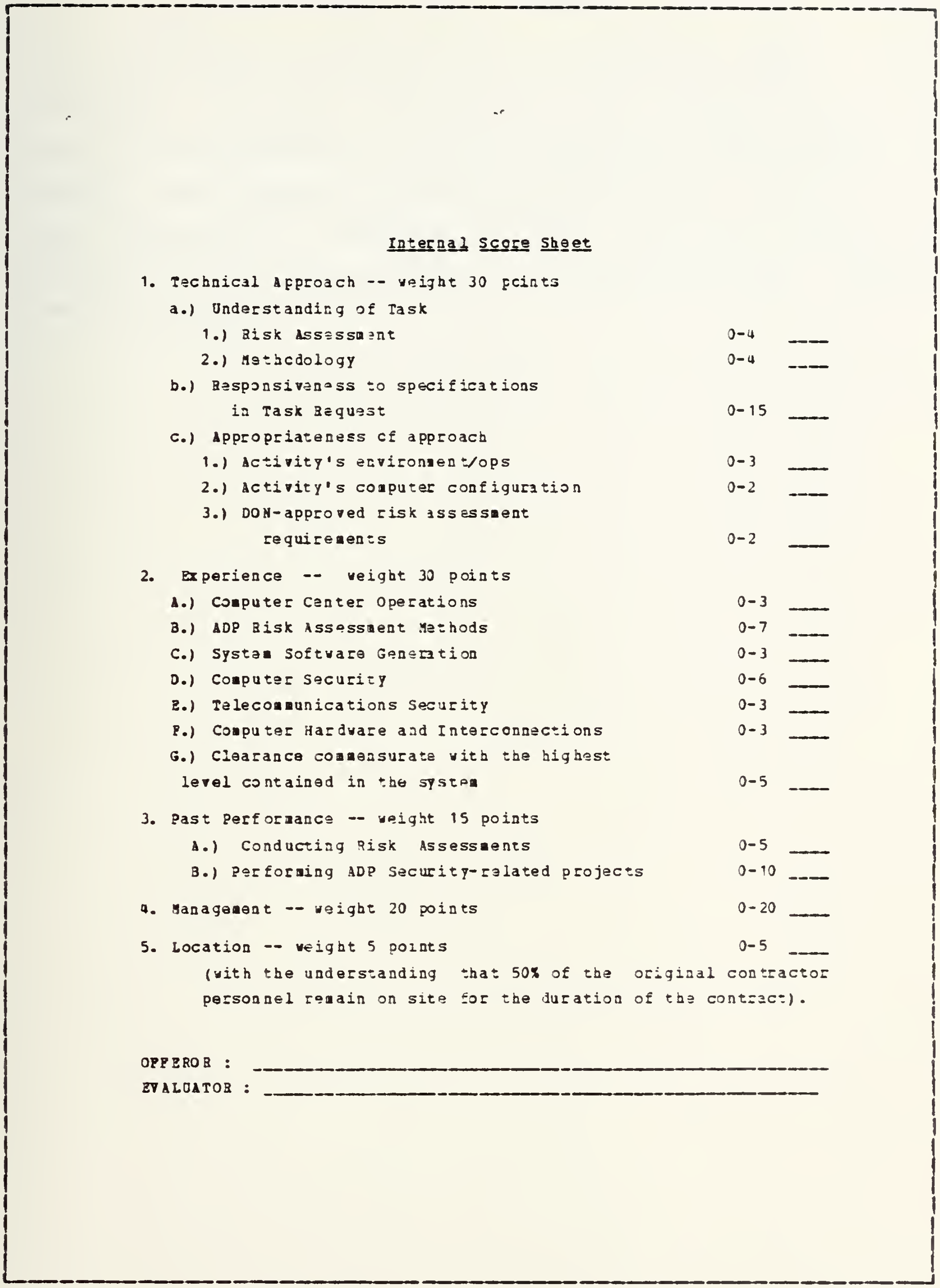
NAVDAC stresses the importance of contractor personnel qualifications in evaluating and selecting the contractor. Particular emphasis is placed on personnel weighting factors, with the result that factors other than cost may weigh heavily in the selection of one contractor over another. The list of qualifications for contractor personnel are quite comprehensive. Particularly important, especially for the lead person assigned by the contractor, is experience in computer center operations, ADP Risk Assessment methods, system software generation, computer security, telecommunications security, and computer hardware and interconnections. A proposal which describes personnel with less than these qualifications may be considered "non-responsive". In order to promote continuity and stability throughout the length of the project, NAVDAC also encourages considering the contractor's response to the requirement that "50 percent of original contractor personnel arriving on a Navy site to perform a risk assessment will remain on site for the duration of the contract" [Ref. 32].

Evaluation of cost factors will generally be handled by the Procuring Contracting Officer of the Navy Regional Contracting Center. This will exclude consideration of the cost of preparing the TOP, which, as is the case with

conventional RFPs, is done at the expense of the contractor. However, those prices which will be recognized include "all direct labor, overhead, general and administrative expenses, plus an amount for profit" [Ref. 32]. In this regard, most risk assessment contracts will probably be of the Cost-plus-fixed-fee type. Based on NAVDAC's general guidance for evaluation factors and weightings, a proposed Internal Score Sheet for any activity's TOP evaluation is included as figure 3.3 . The reasoning for the discrepancy between experience and past performance is as follows : experience in all areas listed is crucial, and while past performance on related contracts would certainly be a desired feature in a contractor, chances are that few will have dealt directly with risk assessments (considering that they are a relatively new requirement). Price factors should constitute about 20 percent of the total weighting. After the contract administrator has completed the negotiations, the selection is made, and "a finalized Task Order will be executed by the contractor and the contracting officer" [Ref. 32].

B. CONCLUSIONS

NAVDAC's recognition of the need for allowing contractor assistance in conducting computer risk assessments is both admirable and realistic. Even if an activity could spare the personnel necessary to conduct a risk assessment, there would undoubtedly be a lack of expertise in the necessary policies and procedures. At this stage of the game, where a risk assessment is still a relatively new and complex phenomenon, few people understand what it is, let alone how to conduct an assessment. (This will undoubtedly change, however, as NAVDAC places more and more emphasis on ADP Security training).



Internal Score Sheet

1. Technical Approach -- weight 30 points

   a.) Understanding of Task

      1.) Risk Assessment 0-4 ____

      2.) Methodology 0-4 ____

   b.) Responsiveness to specifications in Task Request 0-15 ____

   c.) Appropriateness of approach

      1.) Activity's environment/ops 0-3 ____

      2.) Activity's computer configuration 0-2 ____

      3.) DON-approved risk assessment requirements 0-2 ____

2. Experience -- weight 30 points

   A.) Computer Center Operations 0-3 ____

   B.) ADP Risk Assessment Methods 0-7 ____

   C.) System Software Generation 0-3 ____

   D.) Computer Security 0-6 ____

   E.) Telecommunications Security 0-3 ____

   F.) Computer Hardware and Interconnections 0-3 ____

   G.) Clearance commensurate with the highest level contained in the system 0-5 ____

3. Past Performance -- weight 15 points

   A.) Conducting Risk Assessments 0-5 ____

   B.) Performing ADP Security-related projects 0-10 ____

4. Management -- weight 20 points 0-20 ____

5. Location -- weight 5 points 0-5 ____

   (with the understanding that 50% of the original contractor personnel remain on site for the duration of the contract).

OFFEROR : ______________________________

EVALUATOR : ______________________________

Figure 3.3 Contractor Evaluation Score Sheet.

While specific details and samples of contract documents are available to any activity requesting them, NAVDAC encourages tailoring them to the activity's needs. As top management, security personnel, and computer specialists become more educated in the risk assessment phenomenon, the need for such specific guidance will dwindle. In the meantime, government resources will be saved by avoiding the possibility of mismanagement of contracting for computer risk assessments.

IV. A FRAMEWORK FOR CONDUCTING A RISK ASSESSMENT AT NPGS

The Department of the Navy Automatic Data Processing Security Program was recently promulgated by OPNAVINST.5239.1A on August 3, 1982. The instruction provides policy and guidance to commanding officers concerning the establishment of local automatic data processing (ADP) security programs. Each command's program should be designed with the goal of achieving accreditation by the appropriate designated approving authority (DAA). In particular, each activity must develop an activity ADP security plan (AADPSP). This plan must be approved by the Commander, Naval Data Automation Command (COMNAVDAC). The AADPSP should document current security environment, establish program objectives, and outline a plan of action and milestones (POAM) for security program implementation. An item that will be included in the POAM is the completion of a risk assessmemt. A risk assessment may be conducted internally if an ADP activity has the necessary expertise . Commercial assistance is available to conduct a risk assessment. COMNAVDAC maintains a list of authorized contractors and retains approval authority for contractor selection.

This chapter provides a framework for conducting a risk assessment at the Naval Postgraduate School. A framework, in the absence of theory, is helpful in organizing a complex subject, identifying the relationships between the parts and revealing the areas in which further development may be required [Ref. 35]. A risk assessment at a naval activity must be governed, of course, by OPNAVINST. 5239.1A. However, this instruction is very broad in scope and covers the entire ADP security spectrum. It should be helpful to have the necessary steps for a risk assessment , applied to the Naval Postgraduate School, presented in this framework.

A risk assessment involves a detailed examination of all the aspects of a computer system: hardware, software, data, procedures, etc. The use of these assets, that is, the use of the computer systems at the Naval Postgraduate School, including the IBM 3033AP system in the W.C. Church Computer Center, various mini and microcomputers in Spanagel Hall, and independent units obtained under grant by several professors, spans virtually all departments and includes faculty, students, and military and civilian staff. This fact implies that a significant amount of cooperation between different organizations will be required to successfully complete a risk assessment. This endeavor requires command attention at upper levels to impress upon all concerned the importance with which the command views a subject of this nature. With this understanding, a project of this magnitude should produce meaningful results which will serve several purposes:

1) Enable the Naval Postgraduate School to proceed successfully along the path to ADP security accreditation.
2) Provide documentation stating the current condition of security with respect to the computer systems at the Naval Postgraduate School.
3) Provide a reference for quantitatively evaluating security countermeasures.
4) Provide a platform from which improvements in command security posture can be built.

A. INITIAL STEPS: PERSONNEL SELECTION AND SECURITY SURVEY

The initial step in undertaking this project is to identify the personnel who will participate as members of the risk assessment team. Expertise from various disciplines such as computer science, management, and administrative

science will be required. Personnel selection is a very delicate subject in the commercial environment. Donn Parker of the Stanford Research Institute (SRI), at the 1977 National Computer Conference, criticized the concept of a risk assessment team made up of key company personnel. A team approach gives a relatively large number of employees a virtual inventory of data processing vulnerabilities. It may be prudent to have risk assessment team members participate in detailed analyses only on a need-to-know basis. [Ref. 40] However, this situation will not pose a problem at the Naval Postgraduate School. Given the relatively transient nature of students and staff at this institution, the following recommendations for staffing this project are proposed. The position of project manager should be assigned to the ADP security officer. The tasks which this position entails are quite consistent with the duties of the ADP security officer. Additionally, the participation of students from the Computer Systems Management and the Computer Science curricula should be solicited. The majority of the work required in this project could be completed by students. The risk assessment may serve as a thesis project for several teams of interested students. Faculty members of the Computer Council could function in the role of thesis advisors while maintaining an active interest in the risk assessment process. The project could be broken into three distinct phases. Students participating in these phases would build directly upon the work accomplished by earlier students. A proposed phased organization might be:

1) Security Survey, Asset Identification and Valuation Phase
2) Threat and Vulnerability Evaluation Phase
3) Computation of Annual Loss Expectancy and Evaluation and Selection of Additional Countermeasures Phase

The formal assignment of personnel to the Risk Assessment Team is accomplished by the issuance of the Risk Assessment Team Charter. The charter is generated by the command itself and identifies those personnel who compose the team. Since students will be participating in this endeavor, periodic updates to this document will be required. The document lists the objectives of the team and details the authority and responsibility of each person. The charter also states the products which the team is expected to produce.

The next step in the overall process is to conduct an ADP security survey. A sample survey is listed in the ADP Security manual [Ref. 36]. An item which will be needed to ensure that the survey is complete is a listing of all ADP equipment located at the Naval Postgraduate School. The survey should encompass all equipment so that its results can be interpreted with some degree of confidence. The results provide an indication of the current security situation and also may show how much effort will be required to conduct the risk assessment. It should be noted that a complete and accurate listing of all equipment is crucial to the success of the overall assessment. Failure to include certain equipment may invalidate any assessments made on other equipment affected by missing items. The major components of the IBM 3033AP system are listed in an NPGS publication, "Introduction to the Church Computer Center". Of course, this information should be verified prior to use in this endeavor.

The vast majority of the users are not working with high-value data, but rather with routine, academically oriented material. No classified data is supposed to be stored on the IBM 3033AP system. Additionally, most of the processing done at the Church Computer Center is not in support of fleet operations. The results of the survey

indicate some directions for the risk assessment to pursue. The formal results of the survey should be compiled and submitted as an appendix to the risk assessment document.

The results of the survey also impact upon the risk methodology selected. As the ADP Security manual states, "the decision (concerning which methodology to use) should be based on the complexity of the ADP environment. The complexity is governed by the level of data processed, security mode of operation, ADP system configuration and location, and the criticality of the mission." [Ref. 37] There are two methodologies available. The most common methodology for ADP activities is listed in the Security manual as Methodolgy 1. This methodology appears to be suitable for a risk assessment at the Naval Postgraduate School. Methodology 1 is the standard methodology used in most ADP environments and provides for suitable interaction between threats and losses. The risk assessment conducted according to methodology 1 can be divided into several phases as shown in figure 4.1. As previously mentioned, these phases could quite conveniently be assigned to students as thesis projects. The successful completion of each phase is well within the capabilities of interested students.

B. ASSET IDENTIFICATION AND VALUATION

The next phase in this process consists of asset identification and valuation. Some crucial items of information are needed to properly complete this phase. As previously mentioned, a complete, up-to date list of all computer system assets is required. The Computer Council is tasked with maintaining an inventory of all hardware assets [Ref. 38]. They should be able to provide the necessary information in this area. Completeness and accuracy are the

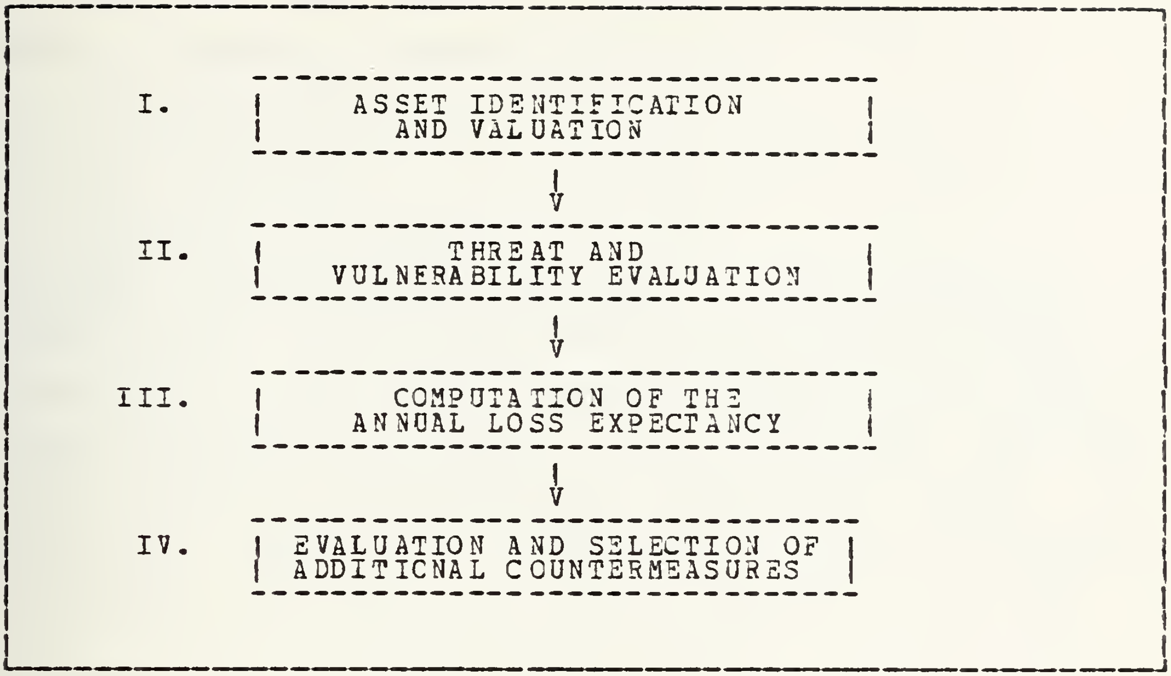

I.
ASSET IDENTIFICATION AND VALUATION
II.
THREAT AND VULNERABILITY EVALUATION
III.
COMPUTATION OF THE ANNUAL LOSS EXPECTANCY
IV.
EVALUATION AND SELECTION OF ADDITICNAL COUNTERMEASURES

Figure 4.1 Major Steps of Method I Risk Assessment.

keys to the success of the risk assessment. Otherwise, the possibility exists that some piece of ADP equipment not listed, and so not considered in the risk assessment, may somehow interact with equipment that is considered. The threat and the associated loss may invalidate the assessments made previously on related equipment.

The other elements crucial to this phase are the impact value ratings. The risk assessment team will determine the impact value ratings. The ADP Security manual gives some general guidance for assigning these values. Since the major purpose of a risk assessment is to provide a quantitative base for evaluating the cost-effectiveness of countermeasures, the importance of these values cannot be overstated. Primary input for the values associated with hardware and software can probably be provided by the computer center staff.

There are four types of impacts for which each asset must be evaluated. These impacts are:

1) Modification
2) Destruction
3) Disclosure
4) Denial of service

The ADP Security manual provides a concise definition of these impacts. Each asset must be evaluated with respect to these items. If an impact affects an asset, then a monetary value reflecting that effect should be assigned. The impact value rating is associated with the monetary value. This stage will require close coordination between the students evaluating the assets and those members of the team who determine the asset impact value ratings. The ADP Security Manual provides guidelines for the impact of disclosure of sensitive data. These values are listed in figure 4.2.

FOR OFFICIAL USE ONLY	$100
PRIVACY ACT OR CONFIDENTIAL	$1000
SECRET	$100000
TOP SECRET	$1000000

Figure 4.2 Sensitive Data Value Guidelines.

There are standard forms which should be used to record the asset impact and valuation studies. The appropriate form for this phase is designated OPNAV 5239/7. An example of this form is provided in Appendix I.

C. THREAT AND VULNERABILITY EVALUATION PHASE

The next phase in the risk assessment process is the threat and vulnerability evaluation. According to the methodology, all threats must be evaluated to estimate how often a "successful" attack may occur. By definition, a "successful" attack is one that results in a definite adverse impact on the activity.

This phase will also require a great deal of communication between the members of the risk assessment team and the staff of the computer center. For certain threats such as power outages, the frequency rating could be determined by examining historical data. However, input from the computer center staff may prove valuable when attempting to determine frequency ratings for threats which are highly technical, such as errors in the operating system software. Each threat must be evaluated with respect to the same four impact areas as the assets, that is, modification, destruction, disclosure, and denial of service. For certain threats which have never, and hopefully will never, occur there may be some difficulty in assigning threat frequencies. There is no sound statistical base for assigning probabilities to human behavior problems. One method to approach this problem is to use the Delphi technique. This method involves having different individuals evaluate a particular probability several times to reach a consensus. This technique should provide a probability estimate which may offset the lack of a human experience base. [Ref. 41]

A great deal of time and effort will be required during this phase. The more imagination which is applied to developing the threats and their potential adverse effects, the more accurate the final risk assessment will be. As a result, the product will serve its purpose and hopefully enhance ADP security.

The ADP Security manual provides a list of several example threats. However, this list is certainly not all inclusive. Threats which are particular to the Naval Postgraduate School computer system, such as the vulnerability of the back-up power supplies and its location on the flight paths of the Monterey County Municipal Airport must be considered . The scope of this risk assessment is all-encompassing. Much imaginative thinking will be required during this phase of the undertaking, however, the payoff in terms of usable output should make it worthwhile. The threats should be defined to minimize overlap. The reason for this concern is generated by the method of computing the annual loss expectancy, which will be addressed in the next step of this phase.

The threat and vulnerability evaluations should also be documented on standard forms. An example of this form, OPNAV 5239/8, is enclosed in Appendix I. The information that should be described for each threat includes a general narrative about the threat. Examples of the threat should be listed and any countermeasures which are currently in effect should be noted. Also, any unique circumstances of the command which might contribute to the threat should be discussed.

As with the previous phase, this portion of the risk assessment could also serve as a thesis project. Again, however, it must be emphasized that close coordination between the risk assessment team and the computer center staff is necessary to ensure that every potential threat is considered and that every frequency rating represents a realistic estimate.

After completing the asset valuation and threat evaluation phases, the next step is to compute the annual loss expectancy values (ALE). This step provides the quantitative results which will be used to evaluate addititonal

security measures. The ADP Security manual describes a mechanical, fairly straight-forward procedure to determine these figures. The impact dollar value ratings and the successful attack frequency ratings interact to produce an annual loss expectancy figure for each of the four impact areas. The individual ALE values for each asset in an impact area and the individual ALE values for each threat in an impact area should be added to produce a total ALE value for each respective impact area. Summing the ALE values over the four different impact areas results in the total ALE value for the system.

As stated in the ADP Security manual, the ALE "represents a quantitative estimate of the potential average yearly financial loss resulting from the modification, destruction, disclosure of data, or denial of services because of existing vulnerabilities which may permit identified threats to be realized." [Ref. 39] One can see that the types of results which are derived, namely, quantitative figures of annual loss expectancy, are based totally upon the estimates made in earlier phases. For the ALE figures to be meaningful, it is clear that a great deal of care must be taken to develop reasonable asset valuations and impact area dollar ratings. Also, the threat evaluation and successful attack frequency must be consistent and not exaggerate any particular area without justification.

D. EVALUATION AND SELECTION OF ADDITIONAL COUNTERMEASURES

After the annual loss expectancy values have been calculated, the evaluation of additional countermeasures can be conducted. The procedure involves determining whether the additional countermeaures would benefit the overall security posture and result in a decrease in the annual loss expectancy value. Cost-effectiveness is the criteria for

decision-making when considering any additional countermeasures. Essentially, every countermeasure must be evaluated to determine if the reduction in the ALE is greater than the cost of installation and implementation. Countermeasures may be directed against specific threats. Some software countermeasures include the establishing of audit trails, the use of unique password/authentication processes, and the imposition of some type of residue control to clear sensitive information which the operating system allows to remain in resource sharing storage. Some hardware countermeasures include the emplcymentof protection state variables, memory protection mechanisms, and the use of interruption resistant power supplies. These are merely a few examples of countermeasures which can be utilized to improve security. They may be such that the successful frequency attack ratings in several impact areas are affected.

The procedure for evaluating additional countermeasures consists of six steps:

1) Countermeasures which can reduce the vulnerabilities of those assets which currently have the higher annual loss expectancy values should be considered first.

2) The vulnerabilities which would be reduced or eliminated by implementing additional countermeasures should be identified.

3) Assuming that the countermeasure is implemented, the projected successful attack frequency ratings for each area should be listed.

4) A projected ALE for each threat affected by the countermeasure should be calculated by impact area.

5) The projected ALE should be subtracted from the current ALE to show the savings possible by implementing the proposed countermeasure.

6) The ALE savings in each impact area should be summed and then divided by the annual cost of the countermeasure to get the Return-on-Investment (ROI). [Ref. 42]

Again, there is a specific form provided to perform these calculations. An example of this form, OPNAV 5239/10, is given in Appendix I.

The Return-on-Investment figure is important in the selection of which additional countermeasure to implement. This selection process occurs in an incremental fashion. As countermeasures are implemented, they affect the overall security posture of the entire computer center. This effect is realized in a different ALE value. Since changes in the ALE will cause a corresponding change in the ROI for a particular countermeasure, the countermeasures must be considered singly.

The countermeasure with the highest ROI is considered first. Then, the countermeasure with the next higher ROI is evaluated with the new ALE resulting from implementation of the previous countermeasure. This procedure is continued as long as the respective ROI remains greater than one. The countermeasures with ROI's greater than one may be ranked according to their respective values. A plan to implement these countermeasures, within budgetary limitations, may then be determined.

The situation may occur where higher authority directs that certain countermeasures be implemented. In that case, these countermeasures may take priority for implementation regardless of their ROI.

V. AUTOMATED VS. MANUAL RISK ASSESSMENT SYSTEMS

A. GENERAL

At this time, no automated or computerized risk assessment methodology has been approved for use by agencies of the Federal Government. This is no reflection on the Government's lack of interest or distrust in the product; it is more a matter of an extremely limited market - there are less than a handful of risk assessment software packages currently available.

One of the few companies in private industry involved in developing risk assessment software is Pansophic Systems, Inc., based in Oak Brook, Illinois. Among the software security products the company offers are : Panaudit, a tool that can be used for ADP, financial, and statistical auditing of computer systems; Panexec, which can be used for auditing, control, backup, and recovery measures; and Panrisk, an automated risk assessment system for management planning. Advertisements for Panrisk boast that it is "...the first system ever to show where to direct your computer security efforts with quantifiable certainty" [Ref. 43].

Although the Panrisk system works under the same basic framework as the manual methods advocated within the DOD, it has a major drawback that greatly limits its usefulness and applicability to government computer facilities. It is only compatible with IBM operating systems. However, if Panrisk had shown any degree of success in the market, other computer vendors would have undoubtedly developed similar systems for Honeywell, Burroughs and others.

According to its advertising brochure, "Basically, Panrisk is the application of a simple formula to a variety of threats whose results are aggregated to give a complete picture of an organization's total loss potential over a period of time " [Ref. 43]. The simple formula for calculating the Annual Loss Expectancy ALE is the same as that given in FIPS PUB 65, although the terminology used differs somewhat:

ALE = single occurrence loss x occurrence rate

ie. impact x frequency

Skeptics might rightfully question using a computer system for such a calculation. Panrisk does, however, produce outputs beyond a simple ALE - it can format, edit, and generate various reports on risk information to be used at all levels within an organization. Thus the package may have some merit in its use as a Management Information System (MIS) or as a Decision Support System (DSS). The problems, though, arise in the input requirements. In order for the system to become useful, the organization must provide the information on its computer resources, threat probabilities, vulnerabilities, and loss potentials. The provision of such inputs constitutes the most difficult part of conducting a risk assessment. Since such inputs are largely based on intuition and experience, it could not be expected that an automated system would be able to produce them. In general, therefore, the market for an automated risk assessment will be extremely limited. In the fall of 1982, Panrisk was taken off the market for an indefinite period of time.

In short, an automated system is no better than a manual one on the input side of the Risk Assessment process.

Furthermore, organizations must exercise caution in considering buying off-the-shelf Risk Assessment software, since Risk Assessments, by their very nature, must be uniquely tailored to an agency's needs. From the standpoint of a DSS, however, an automated Risk Assessment could greatly facilitate a user's understanding and ability to handle budgeting and security problems.

B. A RISK ASSESSMENT AS A DECISION SUPPORT SYSTEM

An automated Risk Assessment could serve as an excellent application for a Decision Support System (DSS). According to Sprague and Carlson [Ref. 44] the characteristics of an effective DSS include : 1.) Support for unstructured (or semistructured) problems; 2.) Support for all levels of decision-making; and 3.) a combination of analytical techniques and data presentation techniques. A Risk Assessment application should include all of these characteristics.

Sprague and Carlson [Ref. 44] discuss three components that make up a DSS : 1.) the dialog model, which serves as the user interface to the system; 2.) the data model, which controls and monitors the system data bases via a data base management system (DBMS); and 3.) the modeling component, which interfaces with the data and dialog models to perform mathematical and analytical operations.

The dialog component of a DSS is perhaps the most important since, from the user's point of view, it functions as a virtual system. The dialog component must be able to support a variety of presentations and output devices, different inputs, dialog styles and communications, and above all, must be user friendly. [Ref. 44] For a Risk Assessment application, this means that the user (possibly the command's Security Manager or ADP Security Officer)

should be able to select the way in which he inputs to the system and the way in which outputs are displayed on the terminal or printer. Inputs, which may include keyboard inputs, joysticks, function keys, etc., will be constrained by the available hardware, but outputs can have several options, largely software-supported, which will only be constrained by the user's and builder's imaginations and abilities. Users may request that the dialog conventions used include question/answer sessions, menu selections, graphical displays, and HELP facilities to aid in supporting the user's knowledge base.

The data component should be able to support a variety of data structures and types, while allowing for easy data access and retrieval [Ref. 44]. This will require an extremely versatile and capable DBMS, but the current state-of-the-art is such that these requirements could be met by a system as simple as DBASE II which is available on most microcomputers. The DBMS of a Risk Assessment application will require that the user be provided capabilities to generate, update, and maintain data bases composed of, at a minimum, threat, asset, and vulnerability information.

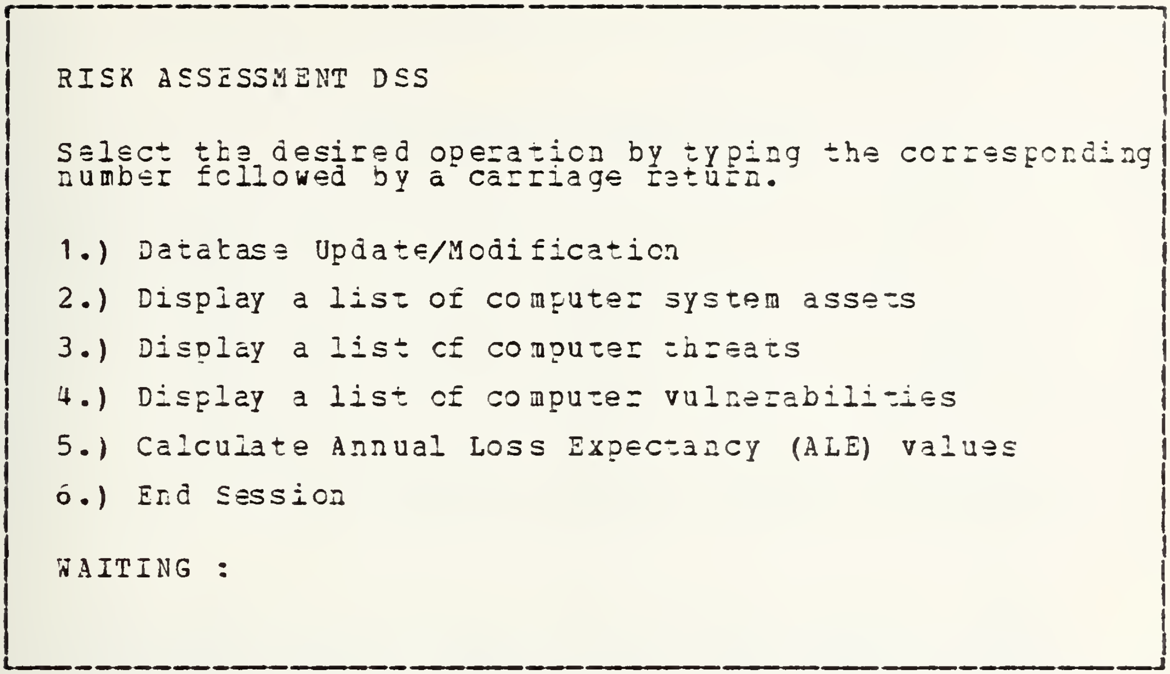
The modeling component must provide a Model Base Management System (MBMS) to allow for the building and creation of new models, model manipulation, and the management of a library of models [Ref. 44]. The models in a Risk Assessment DSS will be used to calculate ALEs for impact and threat categories, compare various ALEs, and mathematically combine and manipulate ALE figures. This component could be handled by the programming capabilities of DBASE II.

C. DESIGN SUGGESTIONS FOR A DECISION SUPPORT SYSTEM

1. The Dialog Component

This component should initially allow the user several presentation options, and should be built such that later refinements and enhancements can be made with relative ease. As the user becomes familiar with the system and feels comfortable in using it, he may want to reduce the system's HELP facilities in favor of more speed and flexibility. Initially, however, the user's knowledge base will be small and he will prefer to be "led through" the system. Assuming the user is at least familiar with how to initialize the system, turn the terminal on and logon, he will then need to know how to make a call to the Risk Assessment DSS. This should be as simple a type-in as "Begin Risk", "Do Risk", or "Risk" followed by a carriage return. The initial screen might look like the one shown in figure 5.1. An additional option might involve moving a cursor below the desired operation using a joy stick, or selecting the operation with a light pen. Once an operation is selected, a new screen showing additional options within that operation will be displayed. All screens beyond the initial one will provide "Help" options as well as options to return to the main menu or end the session. The dialog model might also present the user with a canned list of assets, threats, and vulnerabilities, such that he could delete those that were inapplicable to his organization, and add those that did apply. This would not only serve to increase his knowledge base, but would also prevent a lot of unnecessary terminal work.

Output representations from the operations should come in a variety of formats. Bar graphs might prove to be desirable representations since the user may want compari-



```
RISK ASSESSMENT DSS

Select the desired operation by typing the corresponding
number followed by a carriage return.

1.) Database Update/Modification

2.) Display a list of computer system assets

3.) Display a list of computer threats

4.) Display a list of computer vulnerabilities

5.) Calculate Annual Loss Expectancy (ALE) values

6.) End Session

WAITING :
```

Figure 5.1 Initial Screen for a Risk Assessment DSS.

sons of various ALEs at different periods of time. Figure 5.2 illustrates the type of output representation that might be provided by a Risk Assessment DSS. Similar output representations could be constructed for the other impact areas as well as for threats, assets, and vulnerabilities. For a DSS of this type, most users will desire outputs that show comparisons of relevant information. A prioritized list of vulnerabilities, for example, would show which vulnerabilities are the most costly in terms of ALEs.

2. The Data Component

The Data Component will be perhaps the most difficult to understand and manage. A viable and capable Data Base Management System (DBMS) will be required to maintain the vast number of files, the large sizes of the files, and the links between the files. In general, an effective DBMS should result in reduced costs of building and using the

```
                  Destruction Impact Area


ALE    -100  |
             |
        -80  |             +--+
             |             |  |
        -60  |     +--+    |  |
             |     |  |    |  |     +--+      +--+
        -40  |     |  |    |  |     |  |      |  |
             |     |  |    |  |     |  |      |  |
        -20  |     |  |    |  |     |  |      |  |
             |     |  |    |  |     |  |      |  |
          0  |     |  |    |  |     |  |      |  |
             +-----------------------------------------
                   1979     1980     1981      1982


NOTES: The ALE OF $60K in 1979 represents the value
calculated for the completion of the original ALE.
Due to the addition of the High Speed Communications
System in 1980, the increase in system vulnerabilities
brought about a proportionate increase in the ALE (to
$80K).
Installed countermeasures lowered the ALE TO $50K in
1981. This status was retained through 1982.
Existing plans should decrease the ALE TO $45K by 1983.
```

Figure 5.2 Bar Graph Output Representation.

DSS, increased data control and sharing, and reduced data redundancy. [Ref. 45] In building the DBMS for a DSS, the designer will chose a data model, which is a "method of representing, organizing, storing, and handling data in a computer" [Ref. 46]. The three parts comprising a data model include : 1.) a collection of data structures; 2.) a collection of operations that can be applied to the data structures; and 3.) a collection of integrity rules that define the valid states for the structures. [Ref. 46]

The data structures for a Risk Assessment will vary depending on the type of file. Separate files will, at a minimum, be required for computer assets, threats, and

vulnerabilities. Figure 5.3 shows the fields that might be contained in such files. Such a field structure, however, will obviously result in a great deal of data redundancy. For example, one asset will be exposed to several threats; conversely, one threat may affect several assets. The most wasteful method would be to list every threat affecting a specific asset and include them as part of a record in the asset file. Similarly, every asset affected by a specific threat would be included as part of a record in the threat file. A more logical method of constructing these files would be to link the records in each file together using some type of relational data base model with primary and/or secondary keys.

Within the data model it will be necessary to define a relationship between the asset and threat files such that it can be determined which assets are affected by which threats, and within which impact categories. The fields used for this relation will be the IMPACT CATEGORIES(4) in the asset file, and the IMPACT CATEGORIES AFFECTED(4) in the threat file. By defining this relation, it will be possible to select a specific asset, link it to an applicable threat, and calculate the ALE. This type of linkage could be performed by a JOIN operation. According to Kroenke, "The JOIN operation is used to combine two relations. A value of one attribute in the first relation is compared with a value of an attribute in the second. If the two values have a relationship specified in the join operation, then the tuples of the relations are combined to form a third relation." [Ref. 50] Thus, an asset record and a threat record can be "joined" by issuing a command such as:

```
ASSET(IMPACT CATEGORY(4)=IMPACT CATEGORY(4) AFFECTED)THREAT
```

where the value of the IMPACT CATEGORY field in the asset file is compared to the IMPACT CATEGORY AFFECTED(4) field in the threat file. If the values of the two fields are equal, then the two records can be combined to form a single record. In this way, it can be determined that the record resulting from the JOIN operation contains an asset, an applicable threat from a specific impact category, and the frequency of occurrence for that threat. The ALE can then be calculated by multiplying the impact value times the threat probability.

ASSET FILE :
asset name/asset category/description/impact categories (4)/impact category costs(4)/

THREAT FILE:
threat name/description/impact categories affected(4)/ frequency of occurrence/

VULNERABILITY FILE:
vulnerability name/description/threats exploiting/

COUNTERMEASURE FILE:
countermeasure name/description/cost of implementing/ vulnerabilities affecting/threat frequencies affecting/

Figure 5.3 Field Layout for Required Files.

The operations that will be applied to the data base files should include, but not necessarily be limited to, retrieval, update, modification, combination, and summation. The dialog component should prompt the user for the desired operation, while allowing him to specify such details as file name, field name, etc.

The integrity rules for the field values in the files may be kept relatively simple. Values for impact

category may easily be constrained to the four categories of destruction, modification, disclosure, and denial-of-service. Numeric values may be limited to a relatively wide range of values within certain limits. For example, frequency ratings for threats may contain any decimal value between .000 and .999. ALE values for the destruction category will be equal to the asset replacement cost. By the same token, no asset ALE may exceed its total replacement cost.

3. The Modeling Component

"The modeling component is the primary tool for supporting many of the activities that decision makers will perform in the process of making decisions and solving problems" [Ref. 47]. The decisions and problems for a Risk Assessment application will evolve about the calculation of ALEs, and determining the areas where the greatest ALE reduction can occur. Thus, a library of models, consisting of permanent, ad hoc, user-built and "canned" models [Ref. 47] will have to be made available to the user. The permanent models, those desired by most users, might have the capabilities shown in figure 5.4. In addition to these, model generators should be at the disposal of the users in order that they may generate and structure their own models. Optional models that may be requested involve activities for projection, deduction, analysis, creation of alternatives, comparison of alternatives, optimization, and simulation. [Ref. 48]

4. Integration of Components

"The model base and its management system must be integrated with the dialog directly, to give the user direct control over the operation, manipulation, and use of models" [Ref. 49]. By the same token, there must be a tight

THREAT MODEL :
a calculation, summation, and analysis of the ALEs contributed to by specific threats

ASSET MODEL :
the ALEs attributed to specific assets.

VULNERABILITY MODEL :
an analysis and percentage calculation of the ALEs caused by specific vulnerabilities.

COUNTERMEASURE MODEL :
an analysis of the ALE reductions that might be brought about by the implementation of specific countermeasures.

Figure 5.4 Permanent Model Capabilities.

coupling between the modeling component and the data component. "With this direct linkage, models can be updated as the data values are updated, and modified or restructured when the data have changed enough to require it" [Ref. 49]. The components and the possible linkages among them may be depicted as in figure 5.5.

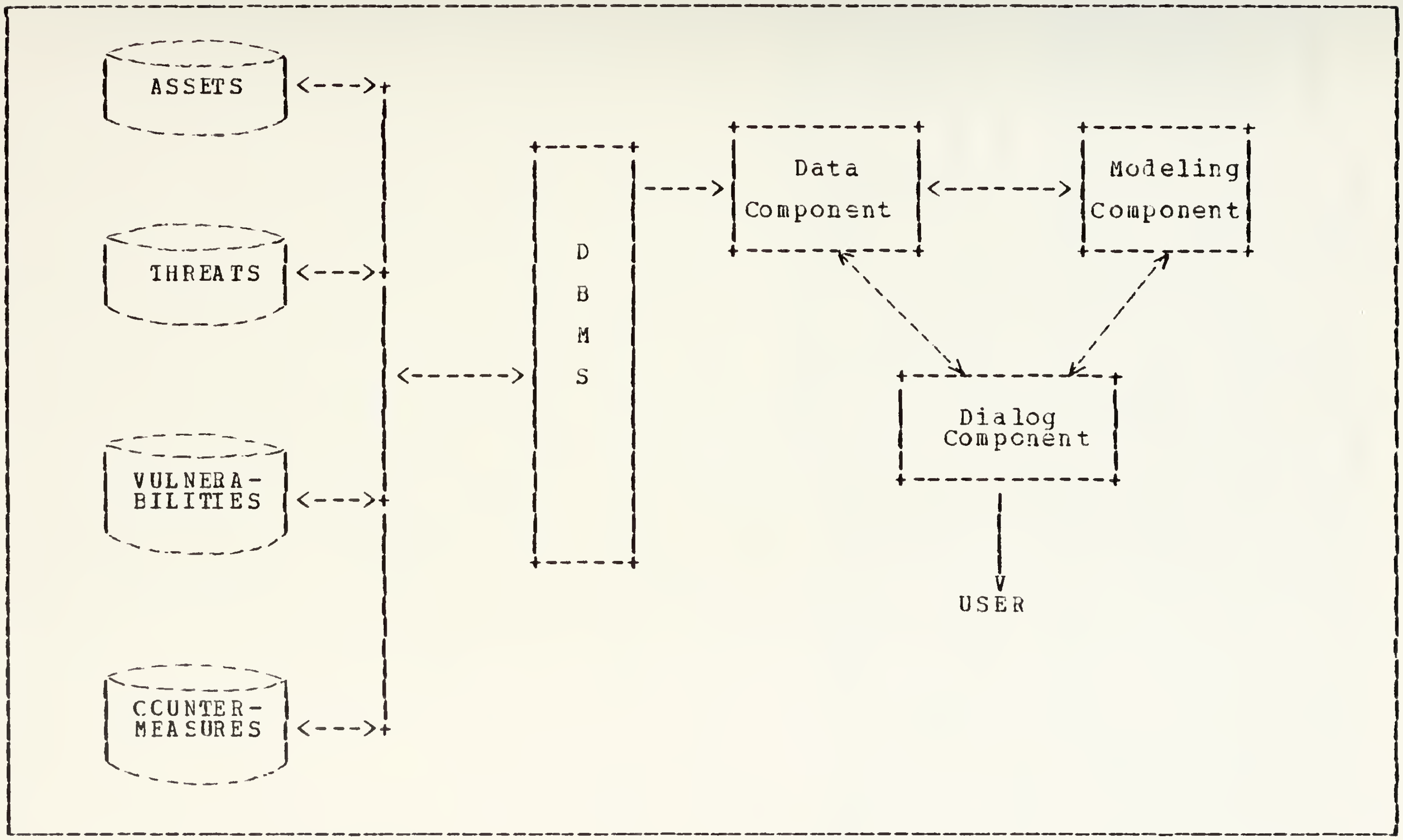


Figure 5.5 Integration of DSS Components.

D. LIMITATIONS

The construction and design of the dialog and modeling components can be made with relative ease. It is in the design and development of the data component that the majority of the difficulties will arise. This will create additional problems in that a complete and capable DBMS is critical to the correct functioning of the dialog and modeling components. The DSS can not function without the complete integration of the three components.

The user is also confronted with severe difficulties in the actual construction of the databases. While the designer may be able to provide an efficient mechanism through which databases may be created and updated, the user may be frustrated in his attempts to collect the data needed to include in the databases.

VI. CONCLUSIONS AND RECOMMENDATIONS

This thesis has examined various facets of the concepts of risk assessment. The subject is exceedingly complex and affects virtually all segments of organizations which employ computers to accomplish their objectives. The multitude of directives promulgated by various agencies of the federal government attest to the attention being focused on risk assessments. The quality of the direction provided in this area is generally good; however, the instructions are often lengthy and sometimes written in a style difficult to follow. The most important point expressed in Chapter Two is the realization that competent guidance concerning risk assessments exists. The level of user awareness regarding the availability of this guidance must be raised. As the federal government in general, and the Department of the Navy in particular, allocate more and more funding to computer systems resources, organizational dependence upon computer services will grow. This fact necessitates a corresponding effort towards ensuring the security of computer systems. For example, the Naval Regional Data Automation Center, San Francisco (NARDAC-SF) allocated several personnel in its Management Control Department to conduct a risk assessment at that facility. Their study resulted in a total annual loss expectancy for NARDAC-SF amounting to over $8.8 billion. It should be noted that an astronomical figure like $8.8 billion in no way represents the actual expected value of losses during a given year. Rather, it is the aggregate ALE resulting from totalling the individual ALE's in each impact area. These figures indicate the relative priorities to be placed on security measures in different areas. Clearly assets evaluated at

relative sums of this magnitude warrant significant security appraisals. This attention and analysis is precisely the driving influence behind the risk assessment directives. Further dissemination to the proper individuals with appropriate authority should increase security efforts in this area.

Several aspects associated with contracting for risk assessment services were considered in Chapter Three. OPNAVINST. 5239.1A directs all commands with computer system assets to conduct a risk assessment. The amount of effort required to conduct a risk assessment may force smaller commands to seek outside assistance. Naval Regional Data Automation Centers (NARDACS) are available to provide assistance. However, the various NARDAC's around the country are staffed at different manning levels, so the amount of assistance each command is able to provide may vary. COMNAVDAC maintains a list of contractors approved to conduct risk assessments or to provide assistance to commands conducting their own risk assessments.

As the framework for conducting a risk assessment at the Naval Postgraduate School demonstrates, the task of actually conducting one is certainly non-trivial. Compiling a list of all systems assets and procedures and assigning impact values to them is a complicated , time-consuming endeavor. Of equal difficulty is determining a list of all potential threats and their associated frequency ratings. It requires personnel experienced in the areas of computer operations, finance and administration. The computation of the annual loss expectancy and its use in evaluating the potential benefits of countermeasures is also an effort which requires a great deal of precision and judgement. The ADP Security Manual provides a reasonably clear explanation of these steps and good background material which is beneficial. The manual also provides examples for each type of computation.

In general, the emphasis currently being devoted to security and risk assessments in the Navy is very timely and prudent. Given the dependence of the Navy on computer technology for such services as supply processing, tracking spare parts failure and usage rates, environmental forecasting, payroll and personnel records and a myriad of other tasks, it is easy to imagine the havoc which could be created if these services are disrupted. The risk assessment program is a positive effort to study the state of security with respect to a command's computer systems, quanitfying the assets and threats and using this data to evaluate countermeasures. The criteria for evaluating countermeasures is cost-effectiveness. The risk assessment procedure appears to be a logical manner in which to determine the relative impacts of various threats on system assets utilizing this criteria.

It would be difficult, if not impossible, to quantify the exact value of the risk assesment itself. Since the overall purpose of a risk assessment is to justify countermeasures in order to prevent disasters, hopefully potential disasters will be averted. Certainly attention will be directed to problem areas in security. However, even though this process has not been quantified, the logic providing the impetus to conduct such assessments seems well-grounded.

No procedure in this area, however, will be successful unless it receives a sufficient amount of command attention. The general tendency for most commands is to treat the security and reliabiltiy of computer services in a "taken-for-granted" manner. The magnitude of the potential disasters due to the loss of computer services makes a change in this type of care-free attitude imperative. The requirement directing all commands with computer systems to conduct a risk assessment is an important, viable means of correcting this attitude. It forces commands to make a

rational, thoughtful analysis of its systems as directed by OPNAVINST 5239.1A. To derive maximum profit from this procedure, the command should ensure that all concerned personnel are aware of the significance of conducting this exercise. If the risk assessment procedure degenerates into a "paperwork drill" conducted by some personnel in the lower levels of the command, then the results may be virtually worthless.

A. SUGGESTIONS/RECOMMENDATIONS FOR IMPROVEMENTS

As mentioned previously, the risk assessment at the Naval Postgraduate School can be completed by students in the various Computer Systems and Management curricula. This situation would provide many benefits of both an academic and practical type, not the least of which are:

1) Provide participating students with a fundamental knowledge of the computer security problem.
2) Save the Naval Postgraduate School a considerable amount of money.

The remaining recommendations are directed at the larger scale problem. A measure which would improve both the efficiency and effectiveness of the risk assessment procedure might be to establish assist teams at NARDAC's throughout the country. These teams would be available to assist commands desirous of conducting risk assessments by providing expertise in security areas not normally encountered by activities as part of their normal routine. The establishment of these teams would serve several purposes:

1) Provide a body of experts to conduct risk assessments and/or to provide assistance to commands conducting them.
2) Enable commands throughout the Navy to conduct their own assessments without being forced to contract for services.

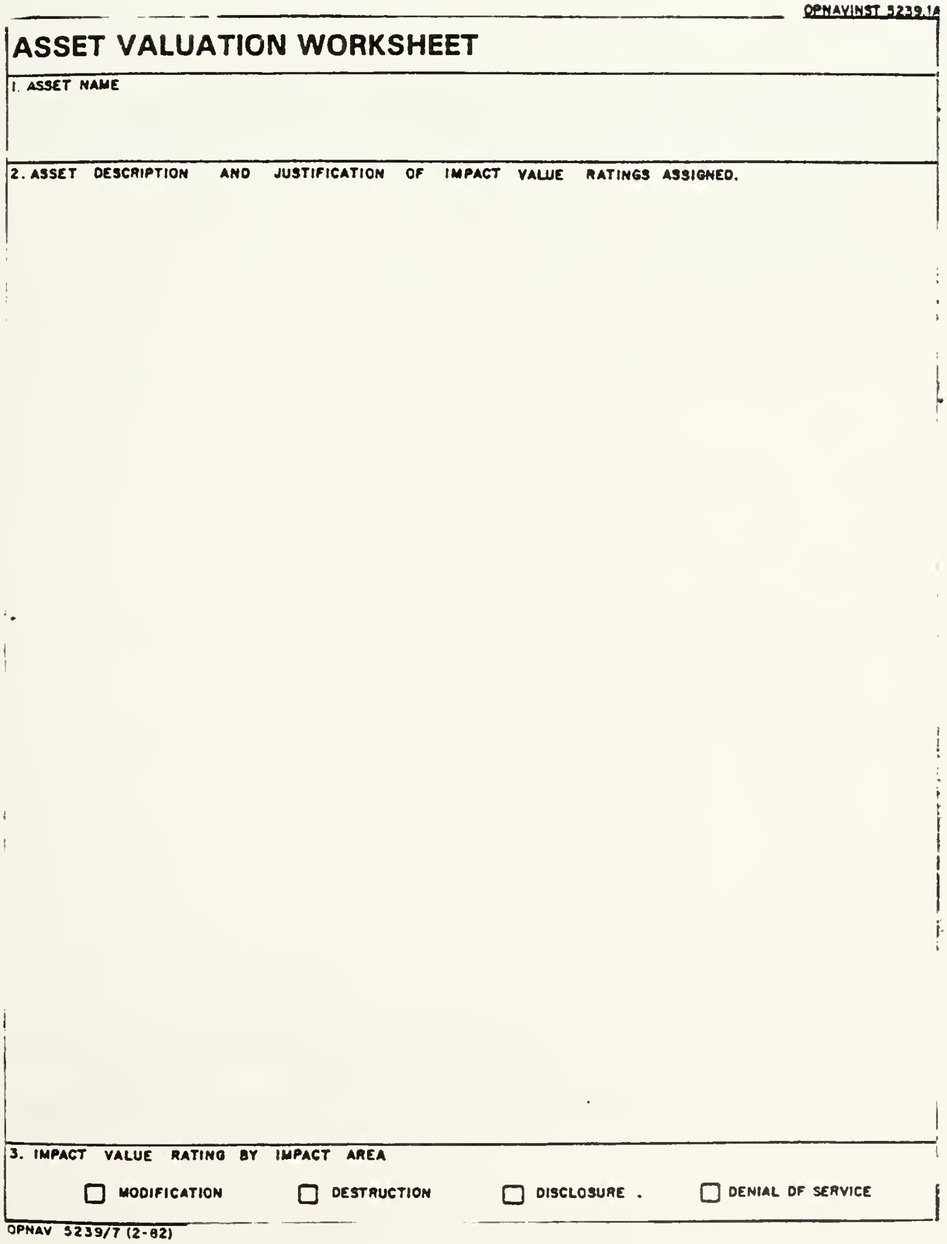
Another area which could be improved is to provide more definitive guidance to commands concerning the value of systems assets. Central agencies in Washington, D.C. such as the Automatic Data Processing Selection Office(ADPSO) and the Naval Data Automation Command(NAVDAC) maintain approval authority and inventories of major systems throughout the Navy. These agencies should possess data concerning the costs of various types of hardware, software, and possibly data. The dissemination of this data could eliminate some of the estimating required to get values for systems assets.

A final recommendation concerns the subject of an automated risk assessment package. Chapter Five has presented the preliminary design for a Risk Assessment Decision Support System. A feasibility study, conducted perhaps at one of the NARDAC's, might be undertaken to assess whether a DSS of this type would be beneficial and cost-effective on a Navy-wide basis. To satisfy a wide range of users, this DSS would have to be extremely user-friendly and capable of accepting a variety of inputs. It may be that the inventory of Navy computer systems is so varied that this type of management support aid would not be practical on such a large basis. However, the potential benefits of this tool merit some investigation.

APPENDIX A

EXAMPLES OF VARIOUS FORMS USED IN RISK ASSESSMENT COMPUTATIONS

This is an example of OPNAV 5239/7.



OPNAVINST 5239.1A

ASSET VALUATION WORKSHEET

1. ASSET NAME

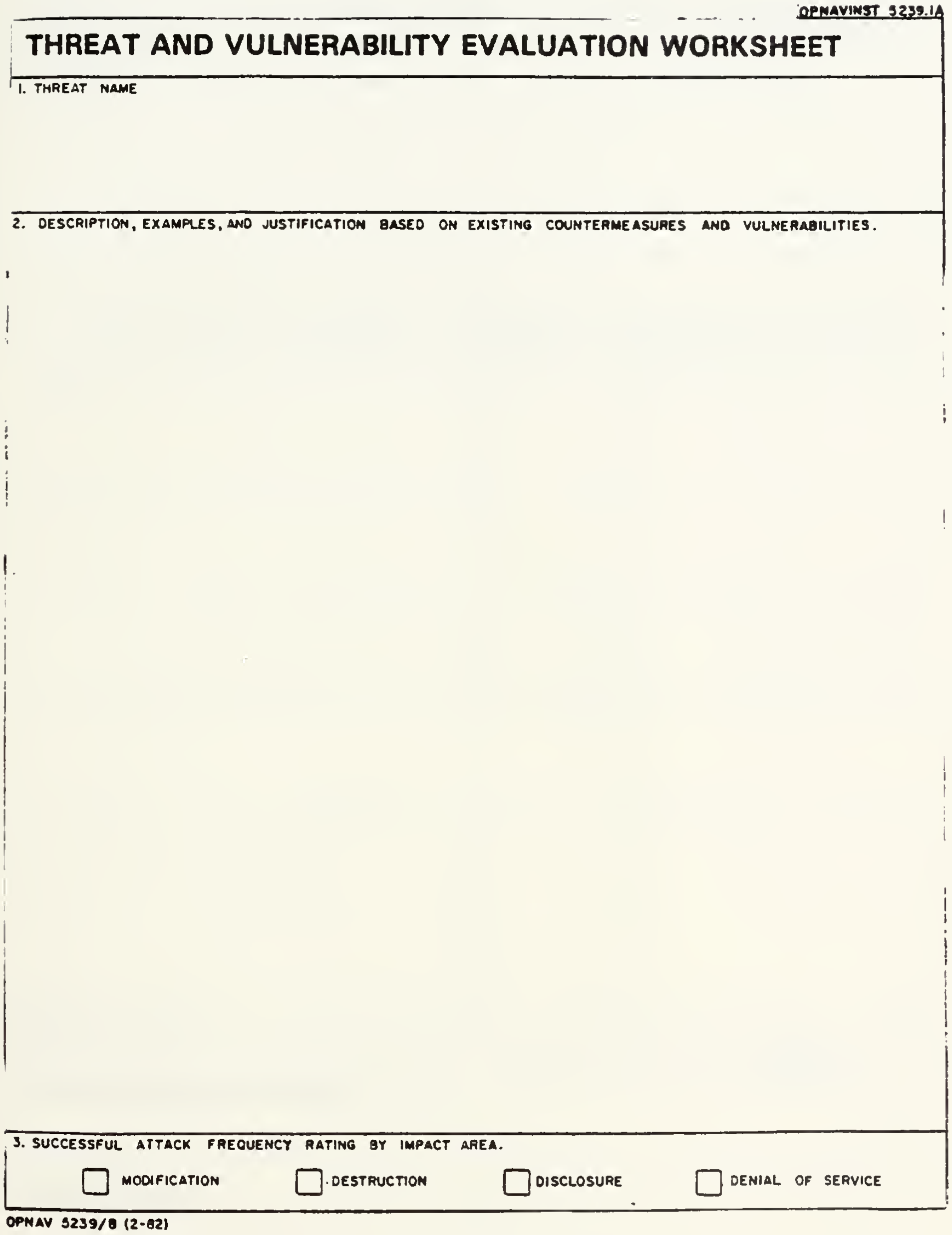
2. ASSET DESCRIPTION AND JUSTIFICATION OF IMPACT VALUE RATINGS ASSIGNED.

3. IMPACT VALUE RATING BY IMPACT AREA

□ MODIFICATION □ DESTRUCTION □ DISCLOSURE . □ DENIAL OF SERVICE

OPNAV 5239/7 (2-82)

This is an example of OPNAV 5239/8.



OPNAVINST 5239.1A

THREAT AND VULNERABILITY EVALUATION WORKSHEET

1. THREAT NAME

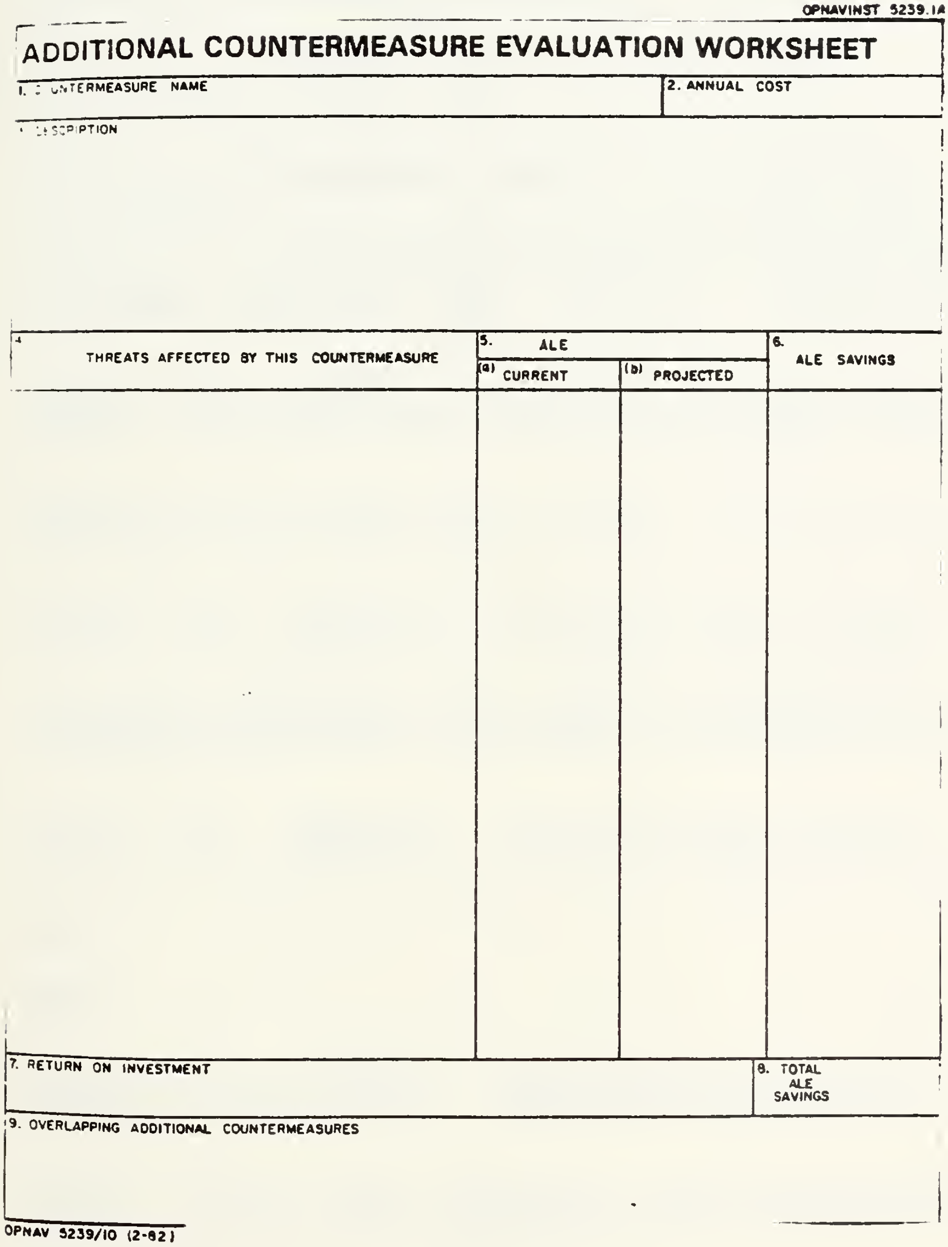
2. DESCRIPTION, EXAMPLES, AND JUSTIFICATION BASED ON EXISTING COUNTERMEASURES AND VULNERABILITIES.

3. SUCCESSFUL ATTACK FREQUENCY RATING BY IMPACT AREA.

□ MODIFICATION □ DESTRUCTION □ DISCLOSURE □ DENIAL OF SERVICE

OPNAV 5239/8 (2-82)

This is an example of OPNAV 5239/10.



OPNAVINST 5239.1A

ADDITIONAL COUNTERMEASURE EVALUATION WORKSHEET

1. COUNTERMEASURE NAME

2. ANNUAL COST

3. DESCRIPTION

4. THREATS AFFECTED BY THIS COUNTERMEASURE	5. ALE		6. ALE SAVINGS
	(a) CURRENT	(b) PROJECTED	

7. RETURN ON INVESTMENT

8. TOTAL ALE SAVINGS

9. OVERLAPPING ADDITIONAL COUNTERMEASURES

OPNAV 5239/10 (2-82)

LIST OF REFERENCES

1. Hammer,C., Managing Computer Security, Computer Security Institute, 1982, p.17.

2. Wylie, T., Organizing for Security, Computer Security Conference, Boston, 1980.

3. Boyer, T., Contingency Planning: An Opportunity For DP Management, Computer Security Institute, 1982.

4. Parker, D., The Potential Effects of Electronic Fund Transfer System on National Security, SRI International, June 1980.

5. Head, R., Federal Information Systems Management: Issues and Directions, The Brookings Institute, 1981, p.4.

6. Office of Management and Budget Circular No. A-71 promulgated 27 July 1978.

7. Browne, P., Security: Computer Center Audits, AFIPS Press, 1979, p.19.

8. Office of Management and Budget, Security of Federal automated information systems, OMB Circular no. A-71, 27 July 1978.

9. Browne, P. Security: Computer Center Audits, AFIPS Press, 1979, pp19-21.

10. Ibid.

11. Ibid.

12. Head, R.V., "Federal ADP Systems : Atrophy in the Sinews of Government", Government Executive, p. 36, February 1981.

13. Haase, W.W., "Data Security Considerations in the Federal Government", Seventh Annual Computer Security Conference, p. 5, November 1980.

14. Department of Defense, Security Requirements for Automatic Data Processing (ADP) Systems, DOD Directive 5200.28, p. 1, 18 December 1972.

15. Office of Management and Budget, *Responsibilities for the maintenance of records about individuals by Federal agencies*, OMB Circular no. A-108, p. 1, 1 July 1975.

16. *Ibid*., p. 13.

17. *Ibid*., p. 3.

18. *Ibid*., p. 6.

19. National Bureau of Standards, *Guidelines for Automatic Data Processing Physical Security and Risk Management*, Federal Information Processing Standards Publication 31, foreward, June 1974.

20. *Ibid*., p. 23.

21. *Ibid*., p. 5.

22. *Ibid*., p. 10.

23. *Ibid*., p. 13.

24. Office of Management and Budget, *Security of Federal automated information systems*, OMB Circular no. A-71, p. 1, 27 July 1978.

25. *Ibid*., p. 5.

26. National Bureau of Standards, *Guideline for Automatic Data Processing Risk Analysis*, Federal Information Processing Standards Publication 65, p. 1, August 1979.

27. *Ibid*., p. 7.

28. *Ibid*., p. 10.

29. *Ibid*., p. 9.

30. *Ibid*., p. 12.

31. Chief of Naval Material, *Contractor Support Services*, *NAVMAT INSTRUCTION 4200.50C*, 1 February 1982, p. 3.

32. Commander, Naval Data Automation Command UNCLASSIFIED Letter COMNAVDAC Ser 50-407/1833 to Commanding Officer, Naval Oceanographic Office, Subject: *Automated Data Processing (ADP) Security Accreditation and Contractor Assistance*, 3 August 1982.

33. Commander, Naval Data Automation Command, *Department of the Navy ADP Security Manual* (*Draft*), NAVDACINST 5510.1X, 1979.

34. Commander, Naval Data Automation Command, *Procedures for Requesting Services from Navy Regional Data Automation Centers (NARDACs)*, NAVDAC INSTRUCTION 5230.1A, p. 2, 13 November 1978.

35. Sprague,R. and Carlsen,E., *Building Effective Decision Support Systems*, Prentice-Hall,Inc., 1982, p.10.

36. OPNAVINST. 5239.1A dated 3 August 1982.

37. *Ibid*.

38. NAVPGSCOLINST. 5400.2A dated 1 April 1982.

39. OPNAVINST. 5239.1A dated 3 August 1982.

40. Fitzgerald, J., *EDP Risk Analysis For Contingency Planning*, EDPACS Newsletter, August 1978.

41. Gerberick, D., *Security Risk Analysis*, EDPACS Newsletter, April 1979.

42. OPNAVINST. 5239.1A dated 3 August 1982.

43. "Introducing Panrisk", Pansophic Systems, Inc., 1980.

44. Sprague,R. and Carlsen,E., *Building Effective Decision Support Systems*, Prentice-Hall,Inc., 1982.

45. *Ibid*., p. 224.

46. *Ibid*., p. 225.

47. *Ibid*., p. 262.

48. *Ibid*., p. 260.

49. *Ibid*., p. 263.

50. Kroenke, David, *Database Processing*, Science Research Associates, Inc., p. 212, 1977.

INITIAL DISTRIBUTION LIST

No. Copies

1. Defense Technical Information Center 2
Cameron Station
Alexandria, Virginia 22314

2. Library, Code 0142 2
Naval Postgraduate School
Monterey, California 93940

3. LDCR Gary Hughes,SC,USN 1
Naval Supply Center Puget Sound
Bremerton, Washington 98314

4. Commanding Officer 1
ATTN: Cdr. E. Perkins
BLDG. 1A
Naval Data Automation Facility
Newport, Rhode Island 02841

5. Lt. Margaret A. Black 2
BLDG. 1A
Naval Data Automation Facility
Newport, Rhode Island 02841

6. CDR. Urbanek 1
Code 44
Naval Postgraduate School
Monterey, California 93940

7. George R. Gill 1
ADP Security, Code 007A
Fleet Numerical Oceanography Center
Monterey, California 93940

8. Lt. Martin F. Doherty 2
Surface Warfare Officer Department Head School
Naval Education and Training Center
Newport, Rhode Island 02841

9. Prof. N. Lyons 1
Code 54LB
Naval Postgraduate School
Monterey, California 93940

10. LCDR. J. Berquist, SC, USN 1
Code 54ZA
Naval Postgraduate School
Monterey, California 93940

11. Naval Postgraduate School 1
Computer Technology Curricular Office
Code 37
Monterey, California 93940

201435

Thesis
B54555 Black
c.1
DoD/DoN requirements
for computer risk
assessments.